∞-Day at Scale: Hijacking Registrars, Defeating 2FA and Spoofing 17,000+ Domains (Even with DMARC p=reject)

PROUDLY MADE BY THESE LAZY ITALIANS

Main Author:
ALESSANDRO BERTOLDI @alesansensei

Contributors for Ideas & Revisions:
ENRICO BERTOLDI @blue screen of death
SIMON PIETRO ROMANO @magictasker
EMANUELE GALDI @musclebyte
GIOVANNI MINOTTI @tranchant

==>Magic, Muscles & Exploits since 2018 <==

Table of contents

Abstract

What happens when a domain registrar becomes the weakest link in your security chain? In this talk, we expose real-world ∞-day (Forever-Day) vulnerabilities that allow attackers to hijack domains, bypass 2FA, and spoof trusted email sources—even with properly configured DMARC p=reject.

Over six years after initial disclosure, these flaws are still exploitable across thousands of domains. We'll demonstrate an attack chain we executed (and successfully repeated one year later) against a major European registrar, Register.it, which serves customers across several countries. By abusing weak password recovery procedures based on self-certification and unauthenticated forms, combined with non-anonymized WHOIS data, we achieved full control of victim accounts—without knowing their credentials or 2FA codes.

We also disclose a critical vulnerability in the N-Able Mail Assure platform (formerly SolarWinds MSP), affecting over 17,000 domains. Authenticated users can spoof **any other tenant**, bypassing SPF and DMARC validations—even when strict rejection policies are in place. This misdesign has remained unresolved since 2018 despite multiple disclosures.

This isn't a story about code bugs. It's about systemic failures—procedural shortcuts, broken assumptions, and regulatory blind spots. These vulnerabilities persist not because they're hard to fix, but because responsibility is diffused and security is treated as optional.

We conclude by proposing a Reliability Scoring System for domain registrars and a browser-integrated "Green Check" trust indicator, aligned with Europe's NIS2 directive and built upon RDAP. These are real, deployable solutions—not theoretical band-aids.

This talk offers a rare, longitudinal view of how neglected design and process flaws allow attackers to operate without malware or exploits—just PDF forms, social engineering, and a little patience.

Introduction

Our research identified severe systemic vulnerabilities in domain registration processes and email security platforms, which attackers can exploit through simple yet devastating social engineering techniques. These critical security gaps span four main attack vectors:

- **Credential Recovery Exploits**: Attackers leverage non-anonymized WHOIS data and weak identity verification processes to hijack registrar control panels, even bypassing Two-Factor Authentication (2FA).

- **Email Spoofing via SPF/DMARC Misconfigurations**: Incorrect SPF/DMARC and inbound policy configurations at major registrars enable attackers to execute sophisticated phishing campaigns targeting thousands of customers.
- **Registrar Impersonation**: DNS misconfigurations and related weaknesses allow attackers to convincingly impersonate registrars, conducting phishing attacks that severely undermine customer trust and domain security.
- **Forever-Day Vulnerability in Mail Assure**: An unpatched, cross-tenant spoofing vulnerability in N-Able Mail Assure (formerly SolarWinds MSP) affects approximately 17,000 domains and bypasses DMARC protection entirely, regardless of configuration. Despite responsible disclosure over six years ago, this critical vulnerability remains unresolved, facilitating widespread email compromise.

Through meticulous testing—including authorized Vulnerability Assessment and Penetration Testing (VAPT) for others major registrars (details withheld due to NDA)—we consistently demonstrated the persistence and severe real-world impact of these vulnerabilities. Our ethical approach, adhering strictly to legal frameworks, underscores the urgent need to address these systemic risks.

Given the evolving regulatory landscape shaped by Europe's NIS2 directive, we propose a significant improvement to the WHOIS successor protocol (RDAP), introducing a standardized Reliability Scoring System and an ICANN-certified visual trust indicator ("green check"). This proposal carefully balances commercial practicality with stringent security standards, aiming to significantly enhance global domain security and user trust.

POC of Public Disclosures and Forever Day (∞-day)

Vulnerability in the Username and Password Recovery Process of Register.it Control Panel/Client Area

Summary

Following a security test performed on a *register.it* account owned by us, we have identified vulnerabilities in the username and password recovery process of the control panel/customer area, made available through the *register.it* website. These procedures, to be used in case it is impossible to access the service due to loss or unavailability of credentials, allow an attacker to deceive customer service into sending both the username and the password reset link via email.

This exploit takes advantage of the lack of Whois anonymization and identification procedures based on the self-certification regulations of the Italian law DPR 8/12/2000 n. 445.

In February 2024, reports were sent to Register S.p.A regarding vulnerabilities identified in their username and password recovery process for the control panel/customer area.

After verifying that our discussions were not productive for over two months, we decided to further investigate the nature of the vulnerabilities and proceed with public disclosure in the last decade of May 2024.

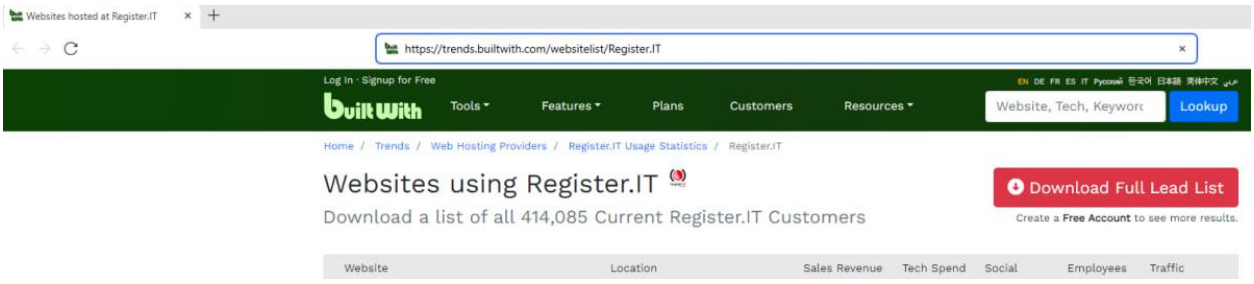
Technical Details

Elements that enable the exploit:

- Lack of Whois anonymization by the domain owner
- Procedures made available online by *register.it*
    - Link to the procedure for sending documentation for password recovery: *https://www.register.it/help/invia-documentazione-recupero-password/*
    - Link to the password recovery form: *https://www.register.it/wp-content/uploads/modulo-recupero-pswITA2020-2.pdf*
- Identification procedures based on the self-certification regulations of Italian law DPR 8/12/2000 n. 445

Proof of Concept (POC) of the exploitation of the elements indicated above:

The attacker can find a complete list of domains belonging to *register.it* using the BuiltWith service and then check their WHOIS information.



<u>Using the non-anonymized Whois, the attackers view the Registrant and Admin Contact data to be used in the online form: *https://www.register.it/help/invia-documentazione-recupero-password/*</u>

In the "Active Email" field, the attackers enter the new email address with which they want to communicate with *register.it* for credential recovery (e.g., *myname.surname@gmail.com*)

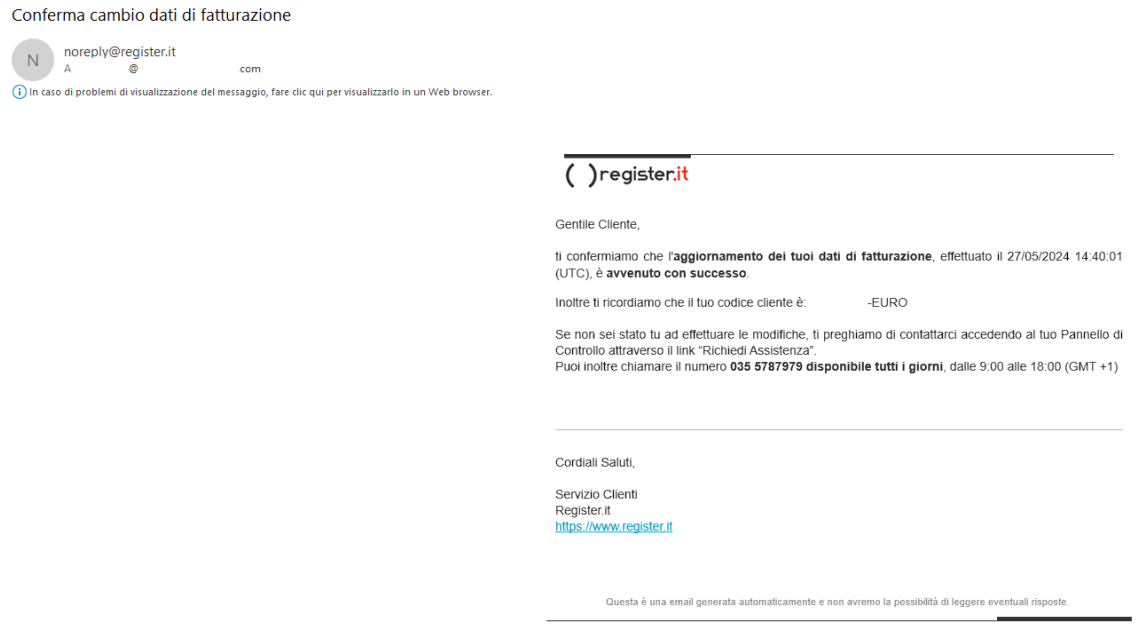
<u>In the "Your message" field, the attackers communicates that they have lost access to the email account used as their username and the password, due to a ransomware attack and request to continue communication at the new email address *myname.surname@gmail.com*.</u>

The attackers fill out the form available at the link: *https://www.register.it/wp-content/uploads/modulo-recupero-pswITA2020-2.pdf*. They obtain the identity document and fiscal code of the Admin Contact through social engineering or by providing false documentation compatible with fiscal code checks.

The attackers send the completed and signed form, identity document, and fiscal code via the upload option on the page: *https://www.register.it/help/invia-documentazione-recupero-password/* after passing the reCAPTCHA.

If the attack is successful, *register.it* contacts the attackers at the provided email with various email communications:

- **Confirmation of the update of billing data and provision of the customer code usable as a username sent to the new email**



Conferma cambio dati di fatturazione

noreply@register.it
A @ com

In caso di problemi di visualizzazione del messaggio, fare clic qui per visualizzarlo in un Web browser.

( )register.it

Gentile Cliente,

ti confermiamo che l'**aggiornamento dei tuoi dati di fatturazione**, effettuato il 27/05/2024 14:40:01 (UTC), è **avvenuto con successo**.

Inoltre ti ricordiamo che il tuo codice cliente è: -EURO

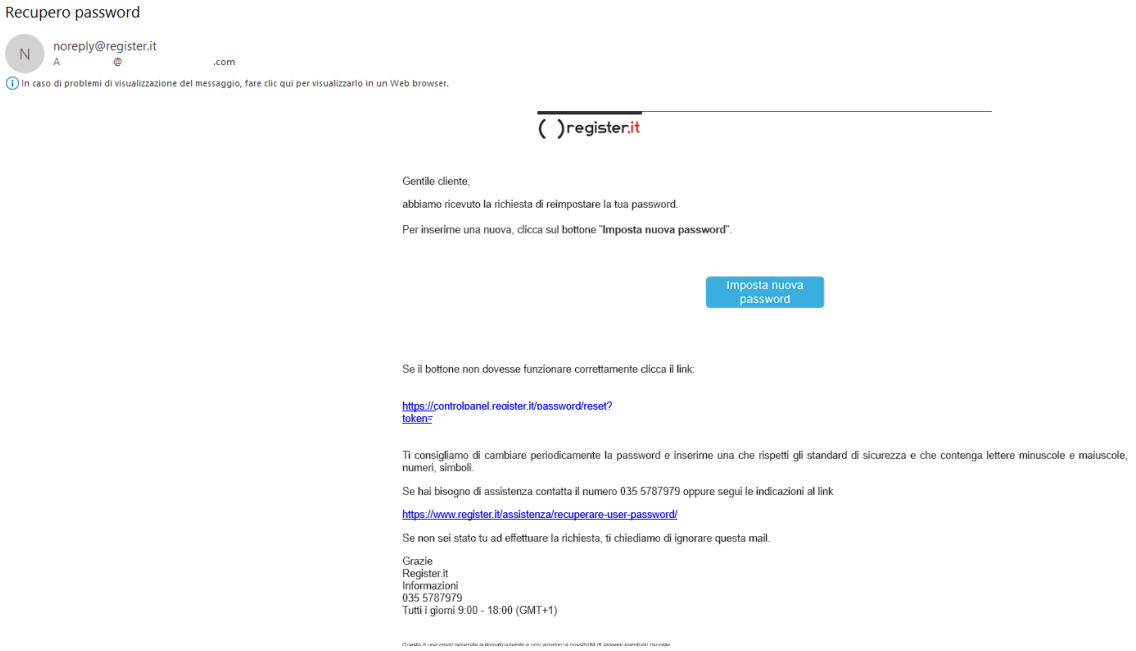
Se non sei stato tu ad effettuare le modifiche, ti preghiamo di contattarci accedendo al tuo Pannello di Controllo attraverso il link "Richiedi Assistenza".
Puoi inoltre chiamare il numero **035 5787979 disponibile tutti i giorni**, dalle 9:00 alle 18:00 (GMT +1)

Cordiali Saluti,

Servizio Clienti
Register.it
https://www.register.it

Questa è una email generata automaticamente e non avremo la possibilità di leggere eventuali risposte.

- **Password reset procedure sent to the new email**



Recupero password

noreply@register.it
A @ .com

In caso di problemi di visualizzazione del messaggio, fare clic qui per visualizzarlo in un Web browser.

( )register.it

Gentile cliente,

abbiamo ricevuto la richiesta di reimpostare la tua password.

Per inserirne una nuova, clicca sul bottone "**Imposta nuova password**".

Imposta nuova password

Se il bottone non dovesse funzionare correttamente clicca il link:

https://controloanel.register.it/password/reset?token=

Ti consigliamo di cambiare periodicamente la password e inserirne una che rispetti gli standard di sicurezza e che contenga lettere minuscole e maiuscole, numeri, simboli.

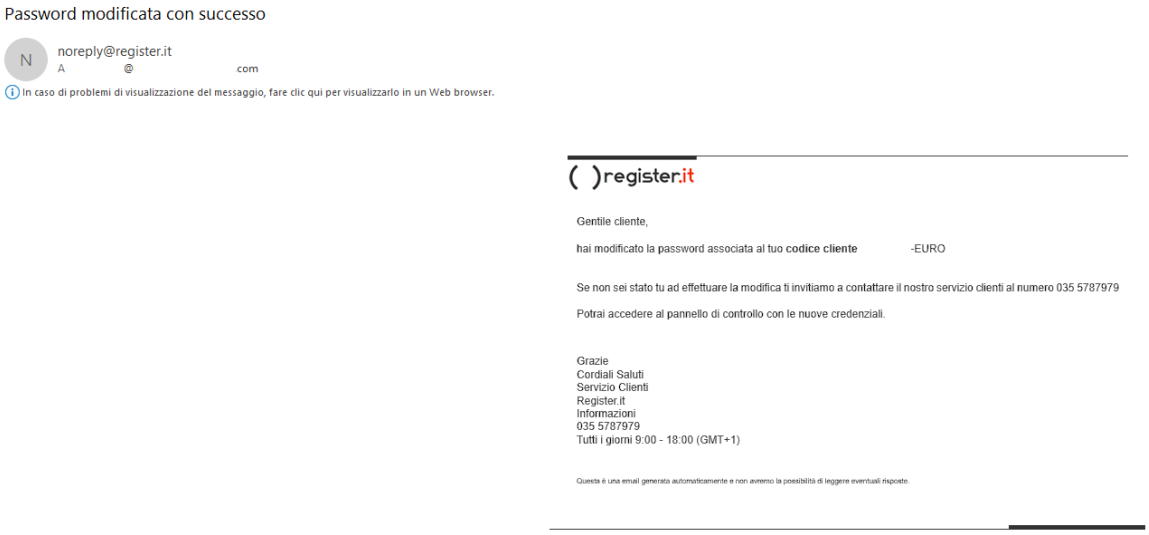
Se hai bisogno di assistenza contatta il numero 035 5787979 oppure segui le indicazioni al link

https://www.register.it/assistenza/recuperare-user-password/

Se non sei stato tu ad effettuare la richiesta, ti chiediamo di ignorare questa mail.

Grazie
Register.it
Informazioni
035 5787979
Tutti i giorni 9:00 - 18:00 (GMT+1)

- Confirmation of successful password change sent to the new email



The attackers can now access the control panel/customer area, taking control of all the target's services.

It should be noted that the Google account previously used to access the customer area of our account (for which the loss of credentials was faked) continues to function without receiving any notification of the password change of the customer area/control panel (which instead arrives at the new email address), leaving the legitimate owner unaware of the ongoing attack and third-party access to the administration panels of their services.

Impact

Ability to modify all elements available on the control panel to carry out further attacks.

For example:

- Ability to modify DNS records and intercept traffic through man-in-the-middle attacks and email interception (using an email gateway that intercepts all mail, archives it, and resends it to the original mailboxes)
- Ability to perform domain theft by generating the Auth-info code.

Recommendations

We strongly advise *Register.it* to implement more rigorous identity verification controls in the credential recovery process as soon as possible, for example by using third-party services for digital verification of one of the following documents: Passport with NFC technology, Electronic Identity Card (CIE), or SPID.

We also recommend all *Register.it* users to anonymize their Whois information and change the data before anonymizing it, if previously made public, in order to avoid attacks on the Whois history that would have the same effect.

Disclosure

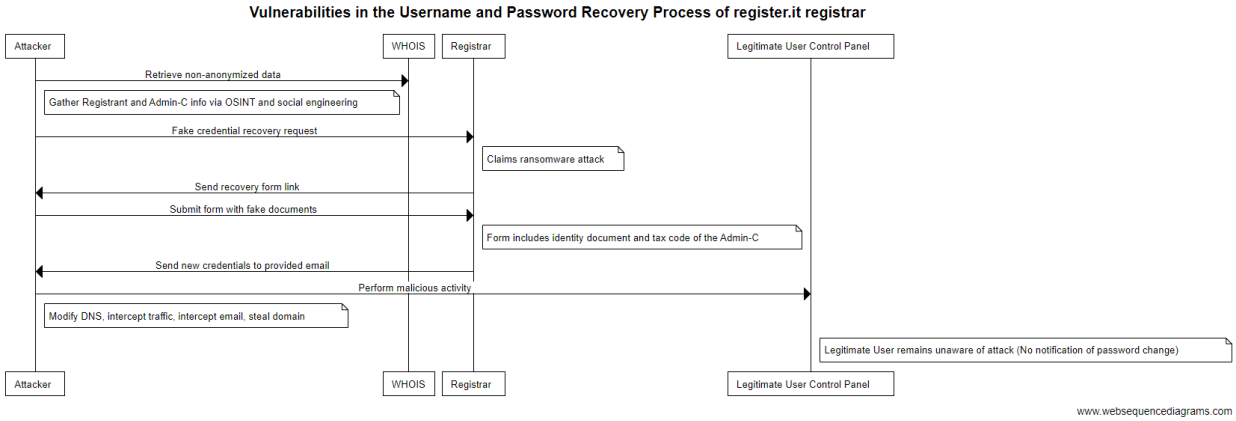
These vulnerabilities were independently discovered and reported to Register S.p.A at the end of February. Although we have noticed the implementation of security controls for onboarding new customers, we assume that adequate actions have not been taken to address the indicated vulnerabilities for all accounts created before our report.

Therefore, it was decided to proceed with a public disclosure to inform *Register.it* customers, particularly those with less recent accounts, and the computer security community in general.

Disclaimer

The Proof of Concept (POC) presented in this document is formulated solely for illustrative purposes to better explain the identified vulnerability. Under no circumstances should it be used for malicious actions or to break any applicable laws. We disclaim any responsibility for improper use of the POC by third parties.

Attack sequence diagram about: Vulnerability in the Username and Password Recovery Process of Register.it Control Panel/Client Area



Cyber Kill Chain

The exploit leverages vulnerabilities in business processes and authentication procedures rather than technical weaknesses in computer systems. Firewalls, antivirus software, intrusion detection systems, and other standard security controls are not designed to detect or block attacks based on social engineering and manipulation of administrative procedures.
This underlines the importance of a holistic security approach that includes not only technical measures but also a critical review and strengthening of business processes and authentication and credential recovery procedures.

Reconnaissance

The attacker uses non-anonymized WHOIS information to view the Registrant and Admin Contact details.
Potential use of social engineering to obtain the Admin Contact's identity document and tax code, or to produce a false document and obtain useful data for impersonation.

Weaponization

The attacker obtains the Admin Contact's identity document and tax code through social engineering or produces false documentation compatible with the checks.
The attacker prepares the password recovery form with false documents or those obtained through social engineering.
Creation of a fake email account to communicate with the Registrar.

Delivery

Submission of the completed form, identity document, and tax code through the online form.

Exploitation

Exploitation of vulnerabilities in the password recovery process of the registrar
Use of non-anonymized WHOIS information and identification procedures
based on self-certification.

Installation

If the attack is successful, the registrar contacts the attacker at the provided email with various communications, including:

- Confirmation of the billing data update.
- Provision of the customer code usable as a username.
- Email with the link for password reset.
- Confirmation of the successful password change.
- The attacker installs the access by gaining control of the credentials.

Command and Control (C2)

From the disclosure: "The attacker can now access the control panel/customer area, taking control of all the target's services."

The attacker establishes continuous control by accessing the control panel and managing the target's services.

Actions on Objectives

From the disclosure: " Ability to modify DNS records and intercept traffic through man-in-the-middle attacks and email interception (using an email gateway that intercepts all mail, archives it, and resends it to the original mailboxes).
Ability to perform domain theft by generating the Auth-info code."

The attacker achieves their objectives by modifying DNS records, intercepting traffic, and potentially stealing the domain.

March 2025: Social Engineering vs. 2FA: How We Bypassed Identity Recovery and Took Over Domains

Summary

Following a security test performed on a register.it account owned by us, we have identified vulnerabilities in the username and password recovery process of the control panel/customer area, made available through the register.it website. These procedures, to be used in case it is impossible to access the service due to loss or unavailability of credentials, allow an attacker to deceive customer service into sending both the username and the password reset link via email.

This exploit takes advantage of the lack of Whois anonymization and identification procedures based on the self-certification regulations of the Italian law DPR 8/12/2000 n. 445.

In February 2024, reports were sent to Register S.p.A regarding vulnerabilities identified in their username and password recovery process for the control panel/customer area.

After verifying that our discussions were not productive for over two months, we decided to further investigate the nature of the vulnerabilities and proceed with public disclosure in the last decade of May 2024.

In March 2025, one year after our initial report, we attempted to repeat the test using the same technique with slight variations, also adding a request to reset the previously enabled 2FA for the control panel account. The test was successful.

The group Register.it, beyond Italy, operates in Spain, Switzerland, United Kingdom and Ireland, France, Portugal, and the Netherlands respectively through the brands Nominalia, Swizzonic, Namesco, Poundhost, Register365, and the Amen Group.

We have not tested the foreign sites, but we expect to find similar issues.

Technical Details

The attacker knows neither the username nor the password nor the 2FA.

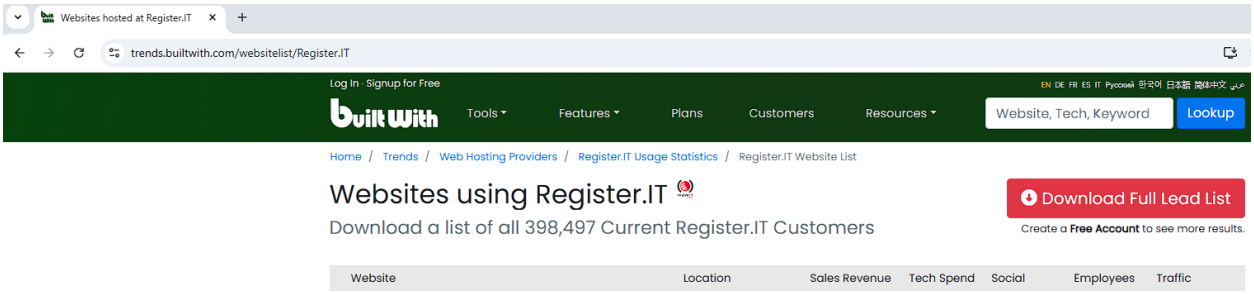
Elements that enable the exploit:

- Lack of Whois anonymization by the domain owner
- Procedures made available online by *register.it*

    - Link to the procedure for sending documentation for password recovery: *https://www.register.it/help/invia-documentazione-recupero-password/*
- Identification procedures based on the self-certification regulations of Italian law DPR 8/12/2000 n. 445 applied both to credential reset and 2FA reset.

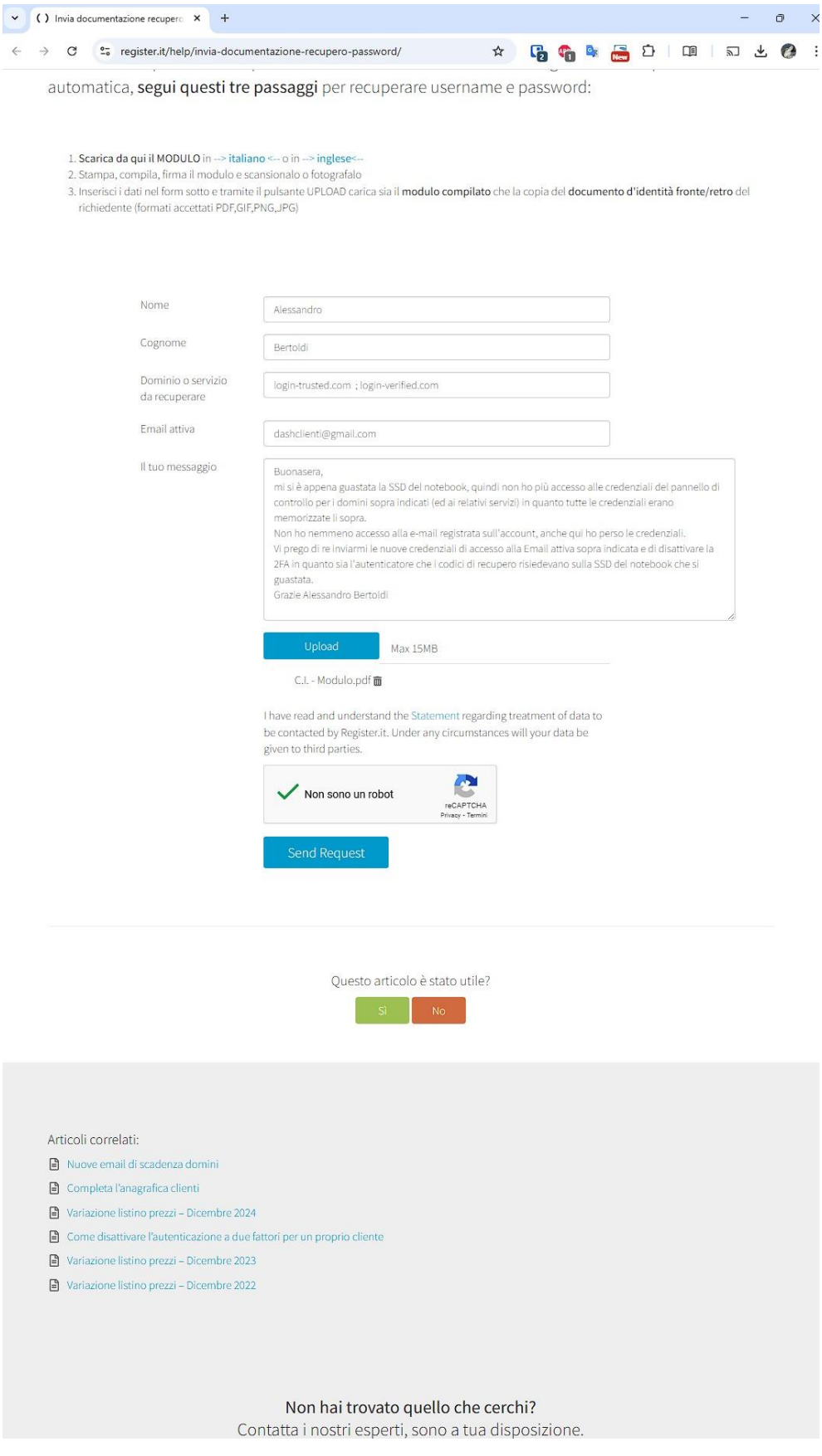
Proof of Concept (POC) of the exploitation of the elements indicated above:

The attacker can find a list of domains belonging to *register.it* to check the WHOIS information using the BuiltWith.com service.



Using the non-anonymized Whois, the attackers view the Registrant and Admin Contact data to be used in the online form: *https://www.register.it/help/invia-documentazione-recupero-password/*

Submission of request by the hostile actor to reset credentials and deactivate 2FA for the control panel associated with the victim's domains using the online form (https://register.it/help/invia-documentazione-recupero-password/), utilizing data obtained from non-anonymized WHOIS and/or through social engineering, as well as a black and white copy of a falsified identity document, or an authentic one also obtained through social engineering with the compiled “request form for control panel access codes” downloaded from the link of the page.


Invia documentazione recuperc
register.it/help/invia-documentazione-recupero-password/
automatica, segui questi tre passaggi per recuperare username e password:
1. Scarica da qui il MODULO in --> italiano <-- o in --> inglese<--
2. Stampa, compila, firma il modulo e scansionalo o fotografalo
3. Inserisci i dati nel form sotto e tramite il pulsante UPLOAD carica sia il modulo compilato che la copia del documento d'identità fronte/retro del richiedente (formati accettati PDF,GIF,PNG,JPG)
Nome
Alessandro
Cognome
Bertoldi
Dominio o servizio da recuperare
login-trusted.com ; login-verified.com
Email attiva
dashclienti@gmail.com
Il tuo messaggio
Buonasera,
mi si è appena guastata la SSD del notebook, quindi non ho più accesso alle credenziali del pannello di controllo per i domini sopra indicati (ed ai relativi servizi) in quanto tutte le credenziali erano memorizzate lì sopra.
Non ho nemmeno accesso alla e-mail registrata sull'account, anche qui ho perso le credenziali.
Vi prego di re inviarmi le nuove credenziali di accesso alla Email attiva sopra indicata e di disattivare la 2FA in quanto sia l'autenticatore che i codici di recupero risiedevano sulla SSD del notebook che si guastata.
Grazie Alessandro Bertoldi
Upload
Max 15MB
C.I. - Modulo.pdf
I have read and understand the Statement regarding treatment of data to be contacted by Register.it. Under any circumstances will your data be given to third parties.
Non sono un robot
reCAPTCHA
Privacy - Termini
Send Request
Questo articolo è stato utile?
Sì
No
Articoli correlati:
Nuove email di scadenza domini
Completa l'anagrafica clienti
Variazione listino prezzi – Dicembre 2024
Come disattivare l'autenticazione a due fattori per un proprio cliente
Variazione listino prezzi – Dicembre 2023
Variazione listino prezzi – Dicembre 2022
Non hai trovato quello che cerchi?
Contatta i nostri esperti, sono a tua disposizione.

In the online form, we entered the victim's first and last name retrieved from non-anonymized WHOIS or through social engineering.
The victim's domain(s), the email address where to continue the conversation, and the following message:
"Good evening, my notebook's SSD has just failed, therefore I no longer have access to the control panel credentials for the domains indicated above (and related services) as all credentials were stored there. I also don't have access to the email registered on the account, as I've lost those credentials too. Please send the new access credentials to the active E-mail indicated above and deactivate the 2FA, as both the authenticator and recovery codes were on the notebook's SSD that failed. Thank you, Alessandro Bertoldi"

We have downloaded the form from the link on the page, completed it, attached a black and white photograph of the identity document, and uploaded it using the upload link on the online form.

( )REGISTER

REQUEST TO DELIVER DASHBOARD CODES

• Complete and sign the declaration, specifying in capital letters and legible writing your name and surname, the name of the service and email address where to send the codes.
• Attach a copy of a currently valid ID document (front and rear) of the applicant.
• Send the request and ID document in **jpg, png, gif or pdf**

The undersigned.....

as legal representative of the company .....

VAT reg. no.....

Which is the domain/service for which the codes are required? (compulsory: specify the name of the service purchased with Register.it)

.....

which address do you wish to receive the access codes?

(enter the email address to which you have access. Do not enter PEC email addresses)

..... @.....

Place and Date Legible signature

....

IMPORTANT:

• ATTACH A COPY OF THE APPLIC ANT ID DOCUMENT

The form was nothing more than a self-certification that repeated the same request as the online form, accompanied by the identity document based on the self-certification regulations of Italian law DPR 8/12/2000 n. 445.

At this point, the attacker is contacted via email by register.it at the new email address previously entered in the online form with a request to send a new hand-signed form for 2FA deactivation and to attach the identity document.
Formally the same previous form but with the addition of the authorization for Register.it to remove the two-factor authentication system.

( )REGISTER

MODULO DI RICHIESTA INVIO CODICI PANNELLO DI CONTROLLO

- Completare e firmare la dichiarazione indicando in stampatello leggibile nome e cognome, il nome del dominio, l'indirizzo email.
- Allegare copia di documento di riconoscimento (fronte e retro) del richiedente
- Inviare richiesta tramite il form, allegando i documenti nel formato **jpg, png, gif o pdf**

Il sottoscritto .....

Con codice fiscale.....

in qualità di legale rappresentante della Società .....

con partita IVA .....

richiedo i codici per il dominio o servizio (in stampatello leggibile)**:**

.....

da inviare all'indirizzo email (NON PEC):

..... @.....

Luogo e data *Firma leggibile*

....

IMPORTANTE:

• ALLEGARE COPIA DEL DOCUMENTO DI IDENTITÀ DEL RICHIEDENTE

☐ **Autorizzo Register.it alla rimozione del sistema di autenticazione a due fattori** (2FA/Two Factor Authentication).

At this point, the attacker uploads the new form with the same data and the same request previously sent to the online form address: https://register.it/help/invia-documentazione-recupero-password/

REGISTER.IT SENDS 2FA DEACTIVATION NOTIFICATION TO THE ORIGINAL EMAIL OF THE DOMAIN OWNER (Is this how register.it is legally protected and disclaims responsibility? Question: does the victim have time to read it?)
Simultaneously, a notification arrives at the new email address entered in the online form by the attacker ("we have removed two-factor authentication and sent the credentials to the email: xxxxxxx@gmail.com" - the email inserted by the attacker)
Simultaneously, a password reset link arrives from register.it's email to the email address entered in the online form by the attacker

After changing the password using the provided link, a notification of successful password change arrives from register.it's email to the email address entered in the online form by the attacker (containing the text "you have changed the password associated with your customer code AB751268-EURO") from which the previously missing customer code needed for logging in can be extracted.

One year after our initial reporting, Register.it has implemented a truly remarkable "security enhancement": simply sending a 2FA reset notification email to the legitimate domain owner.

Meanwhile, an attacker would have already modified DNS records to establish a man-in-the-middle position, effectively compromising the domain. The victim could reactivate 2FA, but the damage would already be done.

What's even more concerning is that throughout this entire process, the Google authentication method previously configured for the control panel remains completely functional and unaffected, despite the credential reset and 2FA deactivation. This means that aside from the notification received from Register.it, the victim can continue accessing their account through Google, completely unaware that their control panel credentials and 2FA have been reset by an attacker who now has parallel access to their account.

Critical Vulnerabilities in Register S.p.A Email Service

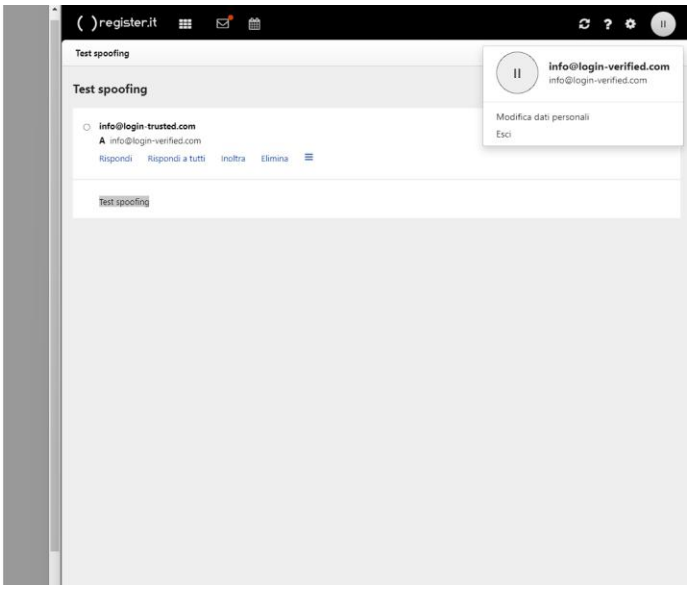
Summary

Following a series of security tests, critical vulnerabilities have been identified in the email service provided by Register S.p.A. These vulnerabilities allow the execution of phishing attacks among *Register.it* customers with standard configuration and by their stakeholders (if they use the SPF qualifier in soft fail for their domain), exposing them to significant risks of computer violations through phishing email attacks. Register's mail system normally receives any email that uses the SPF qualifier set to ~all in DNS, without redirecting it to the Junk Mail folder as it should do according to specifications. In February, reports were sent to Register S.p.A regarding vulnerabilities detected in their email service. After verifying that our discussions were not constructive for over two months, we decided to investigate the nature of the vulnerabilities and proceed with public disclosure in the last decade of May.

Technical Details

To further verify these issues, we regularly purchased the domains *login-verified.com* and *login-trusted.com* from Register, with the associated email services provided by Register in the non-modifiable purchase bundle.

After activating the mailboxes *info@login-verified.com* and *info@login-trusted.com*, we analyzed the SPF record automatically configured on the domain DNS by Register for both mailboxes, namely "`v=spf1 include:spf.webapps.net ~all`". The ~all qualifier specification indicates that if the sender does not match any of the mechanisms listed before the qualifier, the message should be accepted but marked as unreliable. In fact, this happens as per tests we conducted by sending crafted spoofing emails from the domains login-verified.com and login-trusted.com to Microsoft365 and Gmail mailboxes in our possession. However, spoofing is possible between the two domains login-verified.com and login-trusted.com, and this is not due to the ~all qualifier but rather to the lack of adequate inbound policies adopted by register.it regarding the ~all qualifier.



Furthermore, we have identified an additional issue: using Register's webmail, there is a function in the graphical interface used to modify the actual names of the "From" field, but not the real sending email. By activating the "Use custom name" field available within the "Compose" email graphical interface and entering the following data:

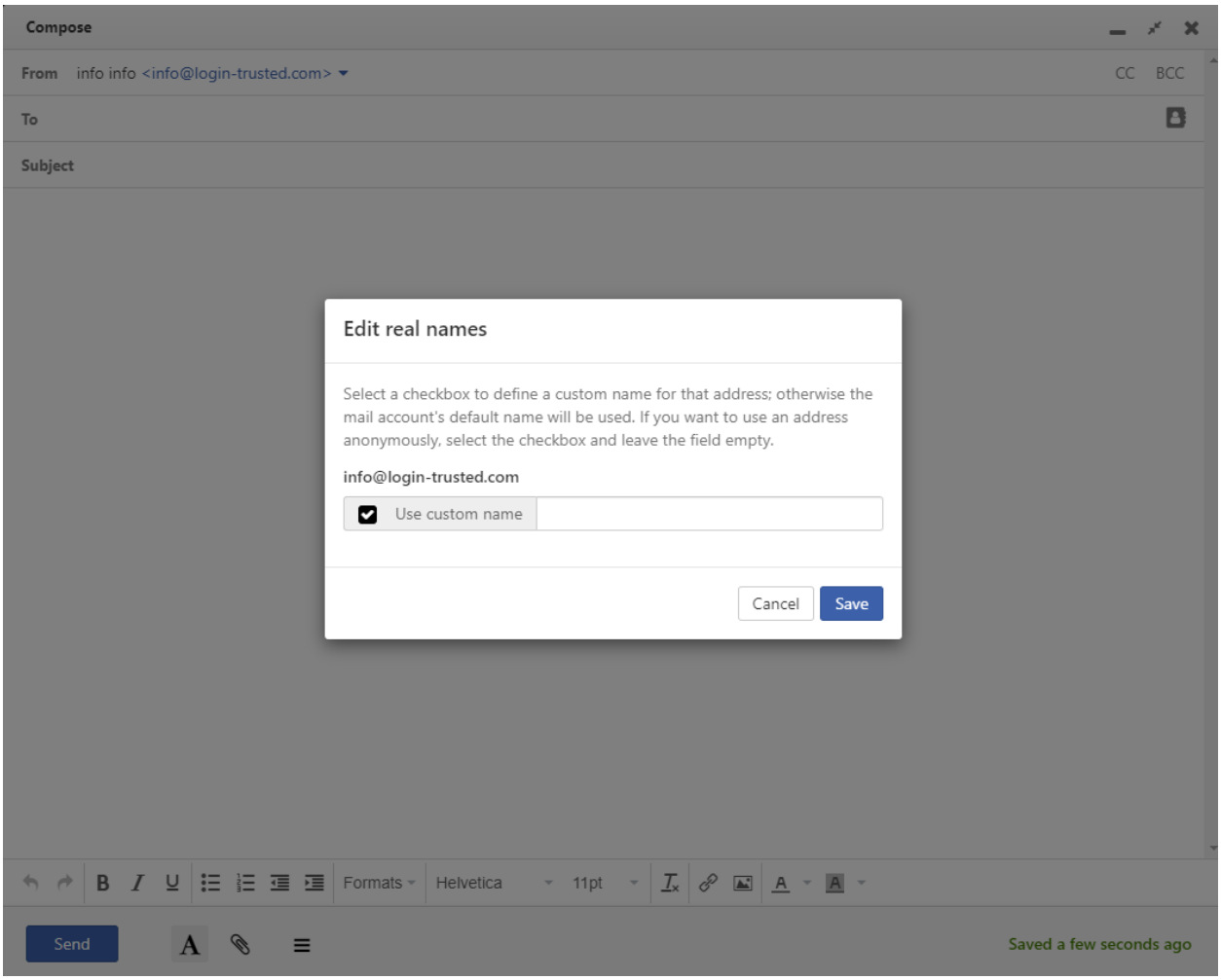
name.surname <name.surname@example.com>

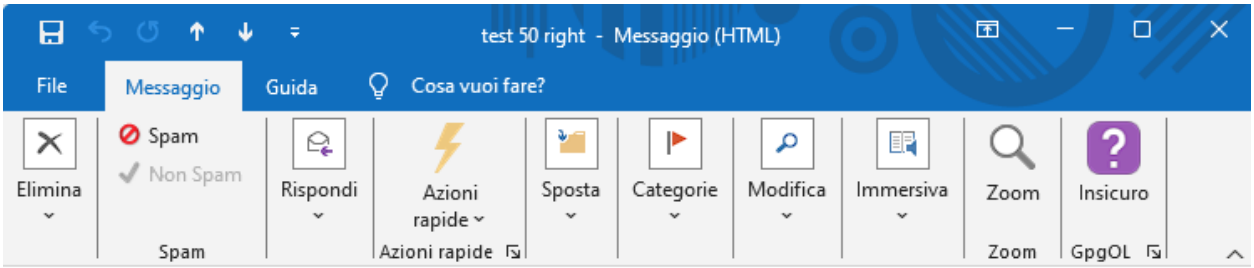
followed by a very large amount of spaces, on the rendering of the "From" field of the recipient's Outlook, it is possible to display as sender

name.surname <name.surname@example.com>

and to move the real sending email address to the right, until it exits the user's visible field, deceiving them about the real origin of the email, all while evading any checks performed by properly configured SPF-DMARC policies.

The artifact works both for domains belonging to register.it and for external domains.





test 50 right

IV

info@login-verified.com

A info@login-trusted.com

Cc ale@bcscompany.it; alessandro@bertoldicybersecurity.com; alessandrobertoldi68@gmail.com

21/05/2024

test 50 right

Impact

Since many Register customers do not change the default SPF configuration automatically inserted by Register, and many domains in general use SPF with the soft fail qualifier, these configurations combined with the weak inbound policy configured on Register's mail system expose its customers to significant risks of attacks and computer violations through phishing emails, using techniques like *BEC (Business Email Compromise)* attacks.
Additionally, the mail server configuration of register.it allows internal spoofing between the domains of customers who use it. This vulnerability is independent of the SPF settings because it pertains to emails circulating within the mail server and presents a significant risk to internal security.

Recommendations

We strongly advise Register to correct the inbound policy so that it accepts the message with the SPF qualifier in soft fail, marking it as unreliable and thus moving it to the user's junk mail folder as it should happen according to specifications. We also recommend for greater effectiveness to set through automatic configuration a default SPF equal to:
`v=spf1 include:spf.webapps.net -all`.

As for the possibility of maliciously modifying the actual names of the "From" field, by the "Compose" interface provided by Register for sending from webmail, it is sufficient to establish that the "Use custom name" field does not accept from user input a number of spaces greater than one.
It is crucial to fix both the webmail interface, the mail server anti spoofing policy and the mail server inbound policy.

Disclosure

These vulnerabilities have been discovered and verified independently. Register S.p.A was informed of these issues in February, but adequate actions were not taken to address them. Therefore, it was decided to proceed with a public disclosure to inform *Register.it* customers, their stakeholders, and the computer security community in general.

Disclaimer

The POC presented is for illustrative purposes only. It should not be used for malicious actions or illegal activities. We disclaim all responsibility for misuse.

Further Vulnerabilities in Register.it Email Service Allowing Phishing Attacks Impersonating Register.it Against Its Customers

Summary

Following further investigations into the previously reported vulnerabilities in Register S.p.A email service (our previous article), new critical issues have been identified that allow sending phishing emails to *Register.it* customers on behalf of *Register.it*. This happens due to erroneous but easily correctable DNS configurations.

Despite *Register.it* stating in the customer area that they are aware of phishing attempts against their users, as indicated by the warning "Phishing Alert: Email Scams in Progress", in our opinion, the company has not applied the necessary standards to effectively prevent such attacks.

Technical Details

When new customers sign up for Register.it, they typically use an email address that is not associated with Register.it's domain (for example, a Gmail or Outlook address). This email address serves as their username for accessing the Register.it customer area and control panel.
We have conducted tests to assess email spoofing vulnerabilities:

For email addresses associated with domains registered through Register.it, we found that spoofed emails from Register.it are correctly filtered into spam folders.

However, for external email addresses (like Gmail or Outlook) used as usernames, we discovered that spoofed emails often bypass spam filters and reach the inbox.

To illustrate this, consider the following example:

A new customer signs up for Register.it using their personal email address, say johndoe@gmail.com. This email becomes their username for logging into Register.it's services. An attacker could potentially send a spoofed email that appears to be from Register.it to johndoe@gmail.com, and this email might not be caught by spam filters.

This vulnerability is significant because these external email addresses are used for important account-related communications and access to the customer's Register.it services. Successful spoofing could lead to phishing attacks or unauthorized access to customer accounts.
This issue is caused by the configurations of the following DNS records belonging to the *register.it* domain:

SPF (Sender Policy Framework) record is unfortunately invalid, as it includes 13 DNS lookups, exceeding the maximum limit of 10 allowed by the specification.

The current configuration is:

```
v=spf1 mx include:musvc.com include:spf.protection.outlook.com
include:send.register.it include:send2.register.it
include:send3.register.it include:send4.register.it
include:mailgun.org include:_spf.emfwd.name-services.com ~all
```

The DKIM (DomainKeys Identified Mail) configuration is correct. However, the DMARC (Domain-based Message Authentication, Reporting & Conformance) policy does not have the Quarantine or Reject policies enabled, which are necessary to effectively protect against phishing. The current configuration is:

```
v=DMARC1; p=none; rua=mailto:dmarc@register.it;
ruf=mailto:dmarc@register.it
```

Impact

These erroneous/missing configurations expose all *Register.it* customers to a high risk of receiving phishing emails apparently coming from *Register.it* to the email corresponding to their username. Attackers could exploit these vulnerabilities to conduct large-scale phishing campaigns, obtaining undue payments as well as payment data (credit cards, etc.).

Recommendations

We strongly advise *Register.it* to take the following corrective actions:

- Correct the SPF record by reducing the number of DNS lookups to a maximum of 10, in compliance with standards, and possibly use the more restrictive -all qualifier.
- Enable Quarantine or Reject policies in DMARC to ensure effective protection against phishing emails.

Disclosure

These additional vulnerabilities were independently discovered and verified. Register S.p.A was informed of these issues, but to date, no adequate actions have been taken to resolve them.

Therefore, it was decided to proceed with a public disclosure to inform Register.it customers and the IT security community of the persistent risks.

Disclaimer

The POC presented is for illustrative purposes only. It should not be used for malicious actions or illegal activities. We disclaim all responsibility for misuse.

March 2025 Retest: Persistent Email Vulnerabilities in Register.it Services One Year After Disclosure

Summary

In March 2025, one year after our initial report, we conducted a comprehensive follow-up assessment of email configuration vulnerabilities in Register.it's services. Our testing revealed that none of the previously identified critical vulnerabilities had been remediated despite the significant time elapsed since our original disclosure in February 2024.

Technical Details

Our March 2025 retest confirmed the persistence of all previously reported vulnerabilities:

1. **Cross-Customer Email Spoofing Vulnerability**:
    - Emails spoofed between domains hosted on Register.it still successfully bypass security controls
    - The inbound mail policy continues to improperly handle the SPF ~all qualifier, failing to flag or quarantine messages that should be marked as suspicious
2. **Register.it DNS Configuration Issues**:
    - Both SPF misconfiguration and DMARC policy weaknesses identified in the original public disclosure remain unchanged
    - These misconfigurations continue to leave Register.it's domain vulnerable to impersonation
3. **Official Support Email Impersonation**:
    - Spoofed emails appearing to come from Register.it's official support addresses can still be sent to Register.it customers
    - While these emails now typically land in spam folders, they still reach the recipients, creating potential phishing opportunities
4. **"Use Custom Name" Vulnerability**:
    - The critical vulnerability in Register.it's webmail interface remains exploitable: When activating the "Use custom name" field in the email composition interface and entering a format like name.surname <name.surname@example.com>

followed by numerous spaces, the recipient's email client of Microsoft Outlook displays only the spoofed sender information while pushing the actual sender address outside the visible field
    - This vulnerability is particularly insidious as it allows attackers to effectively bypass SPF, DKIM, and DMARC protections
    - The exploit is effective against Microsoft Outlook, allowing spoofing of any address even with active DMARC policies in place

Impact

The persistence of these vulnerabilities one year after initial reporting demonstrates:

1. A concerning lack of priority given to fundamental email security configurations
2. Ongoing exposure of all Register.it email customers to sophisticated phishing attacks
3. Continued vulnerability to business email compromise (BEC) attacks
4. Weak implementation of industry-standard email authentication mechanisms

This case study provides compelling evidence for our proposal to establish standardized security scoring systems and regulatory frameworks that would require timely remediation of identified vulnerabilities.

Recommendations

Our recommendations remain unchanged from our original 2024 disclosure, though they now carry increased urgency given the extended timeframe without remediation:

1. Properly configure inbound mail policies to handle SPF ~all qualifiers according to specification
2. Implement strict DMARC policies (p=reject) and correct the existing SPF records
3. Fix the webmail interface to prevent the "Use custom name" exploit by limiting space characters
4. Implement proper sender validation in the mail server

The persistence of these issues highlights the need for broader industry changes as outlined in our research on WHOIS and RDAP protocol improvements and security reliability scoring systems.

Six Years Later: Forever-Day Attacks on Email Security Still Exploiting 17,000+ Domains

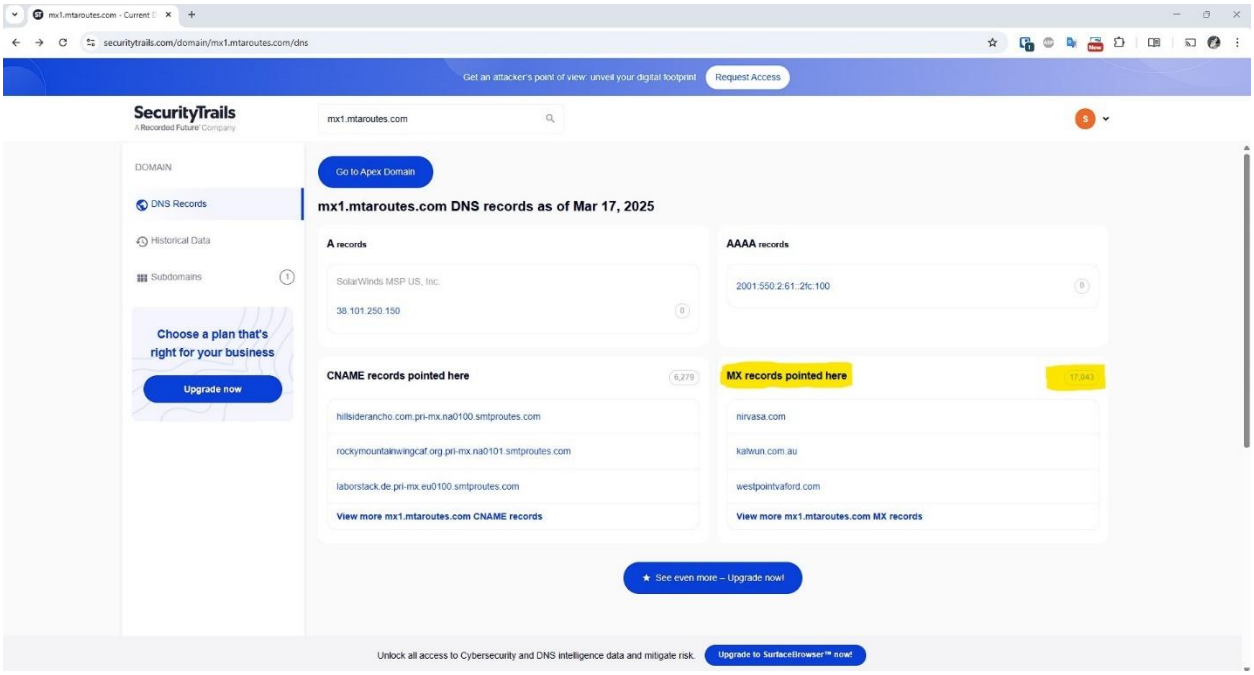
Summary

N-ABLE Mail Assure is a cloud-based email security and archiving platform designed to protect organizations from email-based threats. It provides comprehensive email protection through spam filtering, virus scanning, and phishing defense while offering email continuity and archiving capabilities. The platform is marketed primarily to managed service providers (MSPs) and IT professionals who manage email security for multiple clients.

We are presenting a critical Forever Day (∞-day) vulnerability affecting N-ABLE Mail Assure Platform (https://www.n-able.com/products/mail-assure) ex SolarWinds MSP. This vulnerability was initially discovered and reported to SolarWinds in October 2018, but remains unpatched after more than 6 years, despite formal notification to their security team.

After creating a user account on N-ABLE Mail Assure Platform, the exploit allows an attacker to send emails impersonating any existing mailbox across all domains hosted by Mail Assure, effectively bypassing DMARC protections where implemented.

A preliminary analysis via securitytrails.com indicates approximately 17,084 domains currently rely on this platform, highlighting the extensive potential impact of this vulnerability that has remained exploitable since 2018.

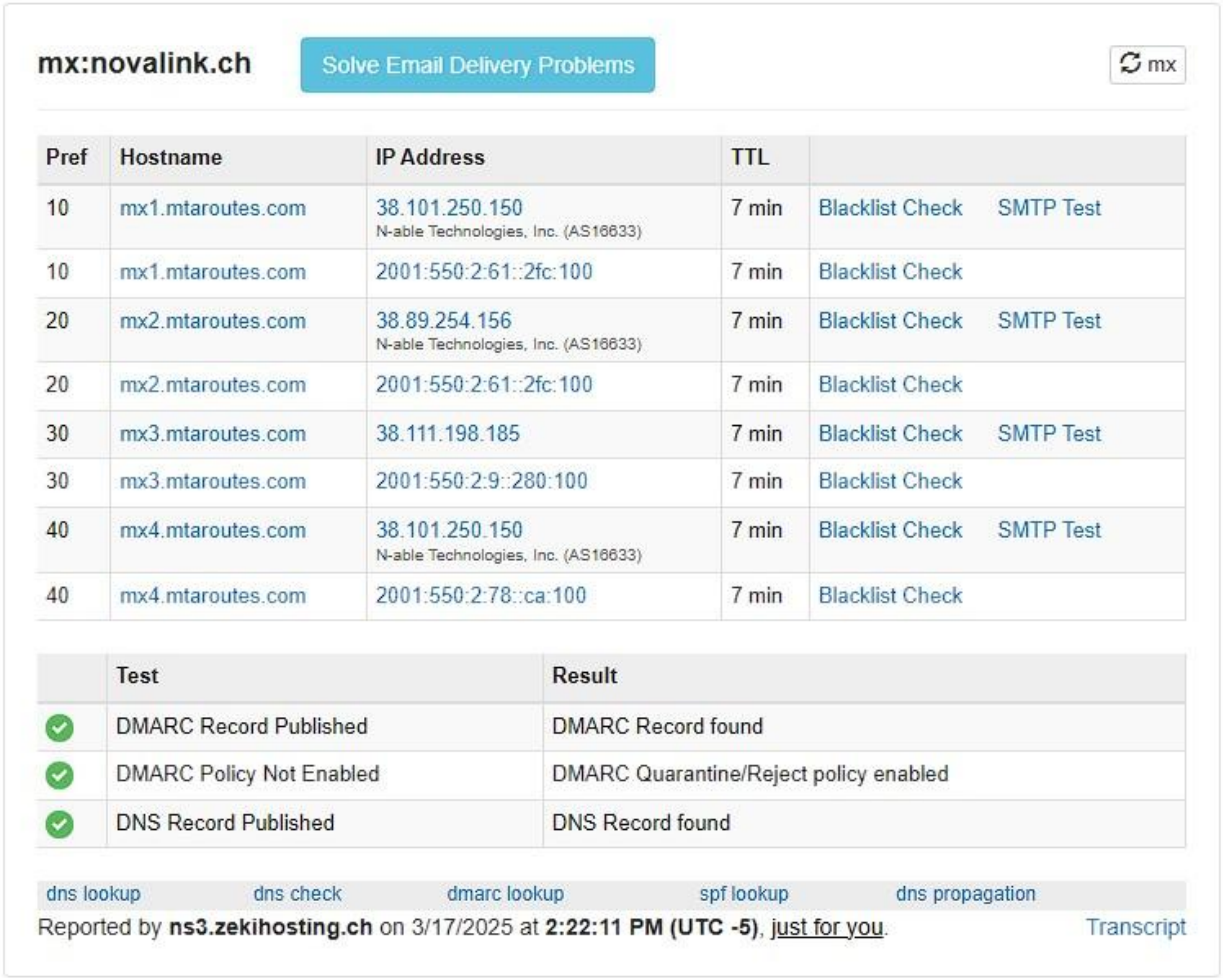


Technical Details

Our research identified a critical authentication bypass vulnerability in N-ABLE Mail Assure that allows cross-tenant email spoofing, effectively neutralizing DMARC protection between tenants using the same service.

To demonstrate this vulnerability, we selected from securitytrails.com service a random domain using N-ABLE Mail Assure with active DMARC protection:

Target domain: novalink.ch (a Swiss IT services company)
The target domain has properly configured DMARC with a strict policy (p=reject), which should prevent spoofing. Their MX records point to N-ABLE Mail Assure servers.



mx:novalink.ch Solve Email Delivery Problems mx

Pref	Hostname	IP Address	TTL		
10	mx1.mtaroutes.com	38.101.250.150 N-able Technologies, Inc. (AS16633)	7 min	Blacklist Check	SMTP Test
10	mx1.mtaroutes.com	2001:550:2:61::2fc:100	7 min	Blacklist Check	
20	mx2.mtaroutes.com	38.89.254.156 N-able Technologies, Inc. (AS16633)	7 min	Blacklist Check	SMTP Test
20	mx2.mtaroutes.com	2001:550:2:61::2fc:100	7 min	Blacklist Check	
30	mx3.mtaroutes.com	38.111.198.185	7 min	Blacklist Check	SMTP Test
30	mx3.mtaroutes.com	2001:550:2:9::280:100	7 min	Blacklist Check	
40	mx4.mtaroutes.com	38.101.250.150 N-able Technologies, Inc. (AS16633)	7 min	Blacklist Check	SMTP Test
40	mx4.mtaroutes.com	2001:550:2:78::ca:100	7 min	Blacklist Check	

	Test	Result
✓	DMARC Record Published	DMARC Record found
✓	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled
✓	DNS Record Published	DNS Record found

dns lookup dns check dmarc lookup spf lookup dns propagation

Reported by **ns3.zekihosting.ch** on 3/17/2025 at **2:22:11 PM (UTC -5)**, just for you. Transcript

```
v=spf1 ip4:194.150.248.68 include:_spf.tophost.ch include:relay.mailchannels.net +a +mx +ip4:
213.180.175.142 +include:servers.mcsv.net +include:spf.mtaroutes.com include:spf.protection.o
utlook.com -all
```

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	ip4	194.150.248.68	Pass	Match if IP is in the given range.
+	include	_spf.tophost.ch	Pass	The specified domain is searched for an 'allow'.
+	include	relay.mailchannels.net	Pass	The specified domain is searched for an 'allow'.
+	a		Pass	Match if IP has a DNS 'A' record in given domain.
+	mx		Pass	Match if IP is one of the MX hosts for given domain name.
+	ip4	213.180.175.142	Pass	Match if IP is in the given range.
+	include	servers.mcsv.net	Pass	The specified domain is searched for an 'allow'.
+	include	spf.mtaroutes.com	Pass	The specified domain is searched for an 'allow'.
+	include	spf.protection.outlook.com	Pass	The specified domain is searched for an 'allow'.
-	all		Fail	Always matches. It goes at the end of your record.

	Test	Result
✓	SPF Record Published	SPF Record found
✓	SPF Record Deprecated	No deprecated records found
✓	SPF Multiple Records	Less than two records found
✓	SPF Contains characters after ALL	No items after 'ALL'.
✓	SPF Syntax Check	The record is valid
✓	SPF Included Lookups	Number of included lookups is OK
✓	SPF Recursive Loop	Nor Recursive Loops on Includes
✓	SPF Duplicate Include	No Duplicate Includes Found
✓	SPF Type PTR Check	No type PTR found
✓	SPF Void Lookups	Number of void lookups is OK
✓	SPF MX Resource Records	Number of MX Resource Records is OK
✓	SPF Record Null Value	No Null DNS Lookups found

```
v=DMARC1;p=reject;sp=reject;adkim=r;aspf=r;pct=100;fo=1;rf=afrf;ri=86400;rua=mailto:zo@novalink.ch;ruf=mailto:zo@novalink.ch
```

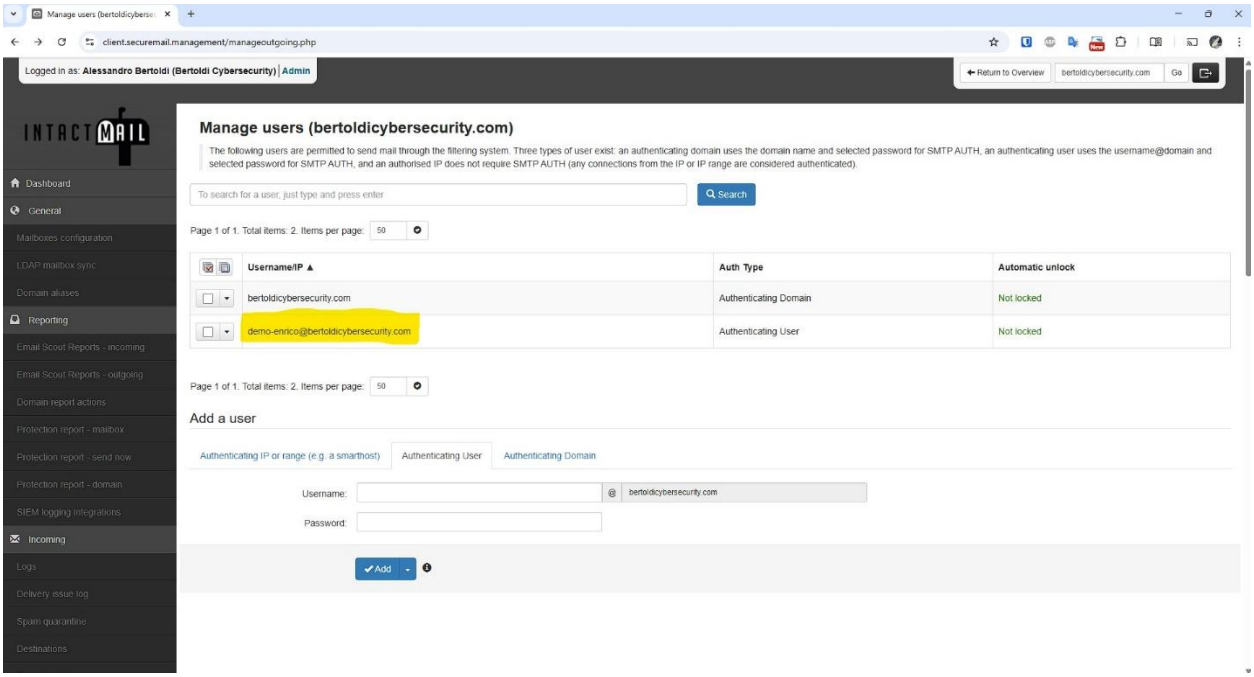
Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	reject	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
sp	reject	Sub-domain Policy	Requested Mail Receiver policy for all subdomains. Valid values can be 'none', 'quarantine', or 'reject'.
adkim	r	Alignment Mode DKIM	Indicates whether strict or relaxed DKIM Identifier Alignment mode is required by the Domain Owner. Valid values can be 'r' (relaxed) or 's' (strict mode).
aspf	r	Alignment Mode SPF	Indicates whether strict or relaxed SPF Identifier Alignment mode is required by the Domain Owner. Valid values can be 'r' (relaxed) or 's' (strict mode).
pct	100	Percentage	Percentage of messages from the Domain Owner's mail stream to which the DMARC policy is to be applied. Valid value is an integer between 0 to 100.
fo	1	Forensic Reporting	Provides requested options for generation of failure reports. Valid values are any combination of characters '01ds' seperated by ':'.
rf	afrf	Forensic Format	Format to be used for message-specific failure reports. Valid values are 'afrf' and 'iodef'.
ri	86400	Reporting Interval	Indicates a request to Receivers to generate aggregate reports separated by no more than the requested number of seconds. Valid value is a 32-bit unsigned integer.
rua	mailto:zo@novalink.ch	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.
ruf	mailto:zo@novalink.ch	Forensic Receivers	Addresses to which message-specific failure information is to be reported. Comma separated plain-text list of DMARC URIs.

	Test	Result
✓	DMARC Record Published	DMARC Record found
✓	DMARC Syntax Check	The record is valid
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.
✓	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled

For our test, we used a legitimate N-ABLE Mail Assure account from an entirely different domain:

Test account domain: bertoldicybersecurity.com

Test account credentials: demo-enrico@bertoldicybersecurity.com



We discovered that when authenticated to the N-ABLE Mail Assure SMTP server (mx1.mtaroutes.com), users can specify ANY sender address in the MAIL FROM command, regardless of whether that address belongs to their own domain or to a completely different domain.

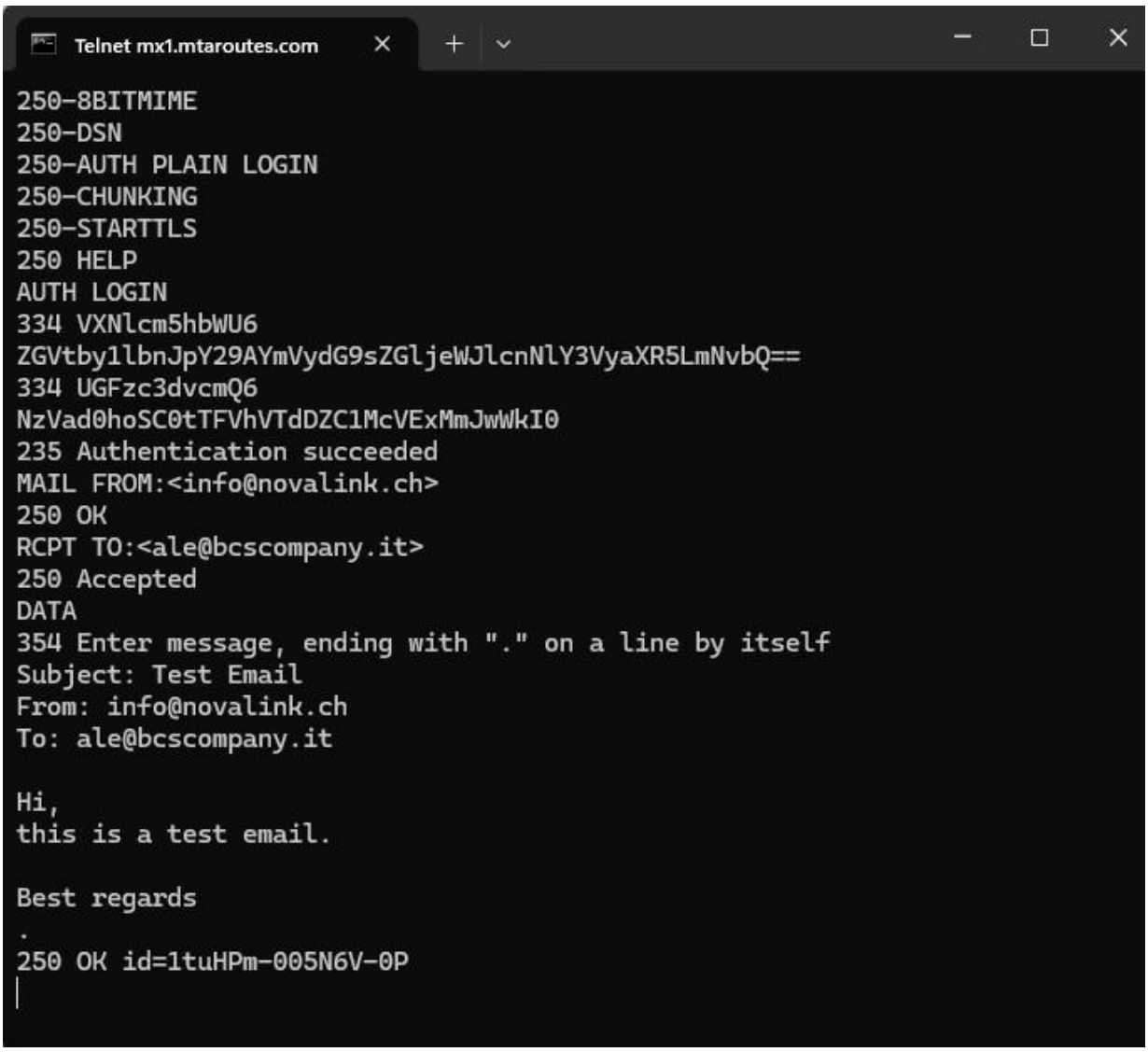
Using a standard telnet connection to the N-ABLE Mail Assure SMTP server, we were able to:

Authenticate using credentials from bertoldicybersecurity.com

Set the MAIL FROM to info@novalink.ch (a completely different domain)

Successfully deliver the message

The exploit works as follows:



To verify that this bypass works in real-world conditions, we sent test emails to both a controlled mail-tester.com address and a production email account.

Clicca qui per visualizzare il tuo messaggio

Da parte di : info@novalink.ch
Bounce indirizzo: info@novalink.ch

- Versione testuale
- Sorgente

SpamAssassin ti ama

Il famoso filtro SpamAssassin. Punteggio: 0.6.
Un punteggio al di sotto di -5 è considerato spam.

-1.396	MISSING_DATE	Missing Date: header
2	RCVD_IN_RP_SAFE	Sender is in Return Path Safe (trusted relay)
-0.001	SPF_HELO_NONE	SPF: HELO does not publish an SPF Record
0.001	SPF_PASS	SPF: sender matches SPF record **Grandioso! Il tuo record SPF è valido**

Non sei del tutto autenticato

Controlliamo se il server da cui stai inviando è autenticato

- [SPF] Il tuo server **185.201.18.98** è autorizzato ad usare **info@novalink.ch**
- Il tuo messaggio non contiene la firma DKIM
- Il tuo messaggio ha passato il test DMARC

Tramite il protocollo DMARC un mittente può specificare se le proprie email sono protette da SPF e/o DKIM, e spiegare cosa fare se entrambe queste autenticazioni falliscono. Ricordati che devi implementare SPF e DKIM prima di utilizzare DMARC.

Il tuo record DMARC è inserito correttamente e il tuo messaggio ha passato il test DMARC
ingresso DMARC DNS trovato per il dominio **_dmarc.novalink.ch**:

```
"v=DMARC1;p=reject;sp=reject;adkim=r;aspf=r;pct=100;fo=1;rf=afrf;ri=86400;rua=mailto:zo@novalink.ch;ruf=mailto:zo@novalink.ch"
```

Dettagli di verifica:

- mail-tester.com; dmarc=pass header.from=novalink.ch
- antispamcloud.com; auth=pass (login) smtp.auth=demo-enrico@bertoldicybersecurity.com
- From Domain: novalink.ch
- DKIM Domain:

- Il server **185.201.18.98** è correttamente associato con **out16-98.antispamcloud.com**
- Il tuo dominio **novalink.ch** è assegnato ad un mail server.
- Il tuo hostname **out16-98.antispamcloud.com** è assegnato ad un server.

Il tuo messaggio potrebbe essere migliorato

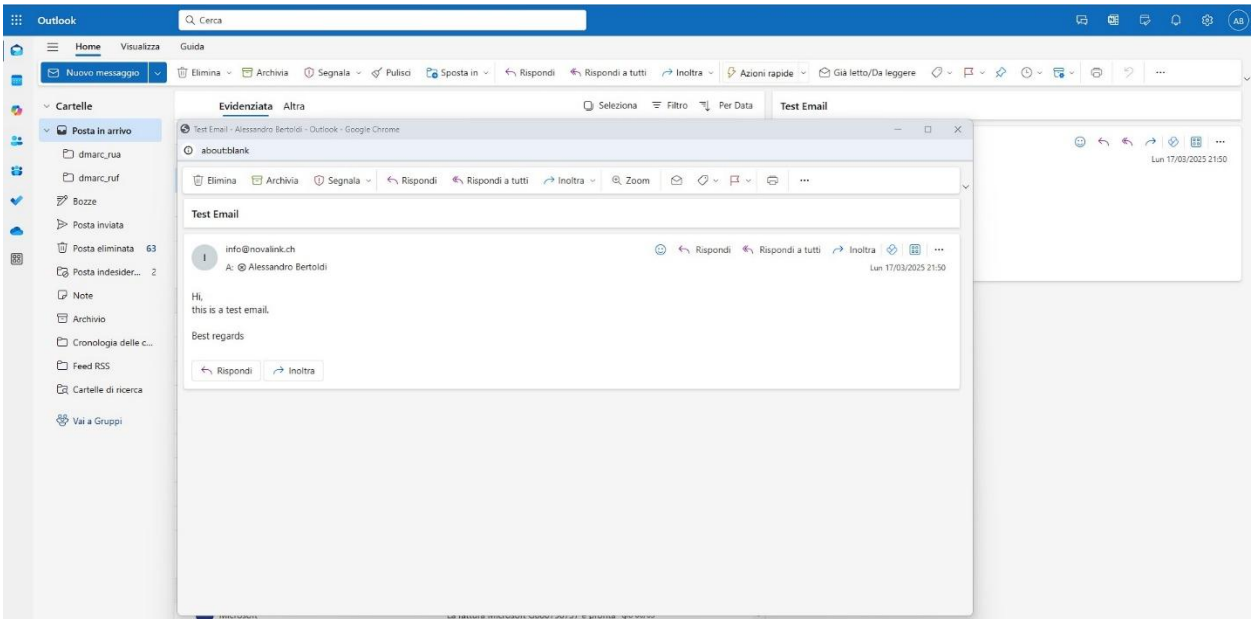
Verifica se il messaggio è correttamente formattato.

Non è presente una versione HTML del messaggio.

- Non sono presenti immagini nel messaggio.
- Il contenuto è sicuro
- Controlliamo se utilizzi un accorciatore URL
- Il suo messaggio non contiene un'intestazione List-Unsubscribe

- Non sei in blocklist

Il tuo amato totale: 9/10



Detailed analysis confirms the message passes both SPF and DMARC checks despite the sender domain (novalink.ch) having properly configured protection.

The root cause appears to be a fundamental flaw in N-ABLE Mail Assure's authentication model, where authentication is tied to the credentials rather than properly validating the sender domain claim against the authenticated identity.

Impact

The vulnerability allows an attacker with valid N-ABLE Mail Assure credentials to spoof emails as if they're coming from OTHER domains that also use N-ABLE Mail Assure - even when those target domains have strict DMARC policies configured to reject such attempts.

This is particularly dangerous because:

It completely bypasses the intended protection of DMARC

It allows cross-tenant spoofing within the N-ABLE Mail Assure environment

The attack works against domains that have properly secured their email authentication

This vulnerability affects approximately 17,043 domains as of March 2025, creating significant risk for business email compromise (BEC) attacks, phishing, and social engineering against organizations that believe they're protected by their DMARC policies.

Recommendations

To mitigate the risks associated with this vulnerability, we strongly recommend the following immediate actions for N-ABLE:
Anti spoofing mechanism

Enforce Domain-based Authentication:

Implement strict validation of the MAIL FROM address against the authenticated account domain.

Ensure that users can only send emails from domains they explicitly own or manage.

Patch the Authentication Bypass:
Modify SMTP authentication logic to prevent cross-tenant spoofing.

Introduce additional checks that validate the sender domain against the authenticated identity before allowing message relay

Enhance Logging & Monitoring.
Implement detailed logging for cross-domain email attempts.
Notify administrators of suspicious cross-tenant email activities in real time.

Disclosure

We are disclosing here a "Forever Day (∞-day)" vulnerability in N-ABLE Mail Assure, which as of March 2025 affects 17,043 domains. This vulnerability was originally discovered and reported to SolarWinds (former owner of Mail Assure product, now N-ABLE) in October 2018 by Bertoldi Cybersecurity Team. Despite formal notification sent to SolarWinds' VP Security Timothy Brown and the company's PSIRT team, this vulnerability has remained unresolved for over 6 years, qualifying it as a true "Forever Day."

The documented correspondence from 2018 (We have documentation on file for this Case) confirms that:

1. The vulnerability was identified during a penetration test of the IntacMail system (our e-mail system base on Mail Assure and Kerio Connect)
2. The email spoofing issue was explained in detail to the SolarWinds security team
3. Assistance was offered for verification and mitigation of the vulnerability
4. Despite confidentiality commitments, the issue remained unresolved

Additionally, in March 2025, we identified and reported another security concern: the lack of DNSSEC implementation on antispamcloud.com domain used by Mail Assure for sending emails. This represents a fundamental security gap in the service's DNS infrastructure, potentially allowing for DNS poisoning attacks. Despite acknowledging the issue (We have documentation on file for Case #02626422), N-Able's response indicated that while they recognize the importance of DNSSEC, they consider it unnecessary for their current functionality since they don't support DANE. This reasoning disregards the broader security benefits of DNSSEC beyond DANE support, including protection against cache poisoning and ensuring DNS record authenticity - critical safeguards for an email security service. This demonstrates a concerning pattern of prioritizing functionality over fundamental security practices.

Disclaimer

The POC presented is for illustrative purposes only. It should not be used for malicious actions or illegal activities. We disclaim all responsibility for misuse.

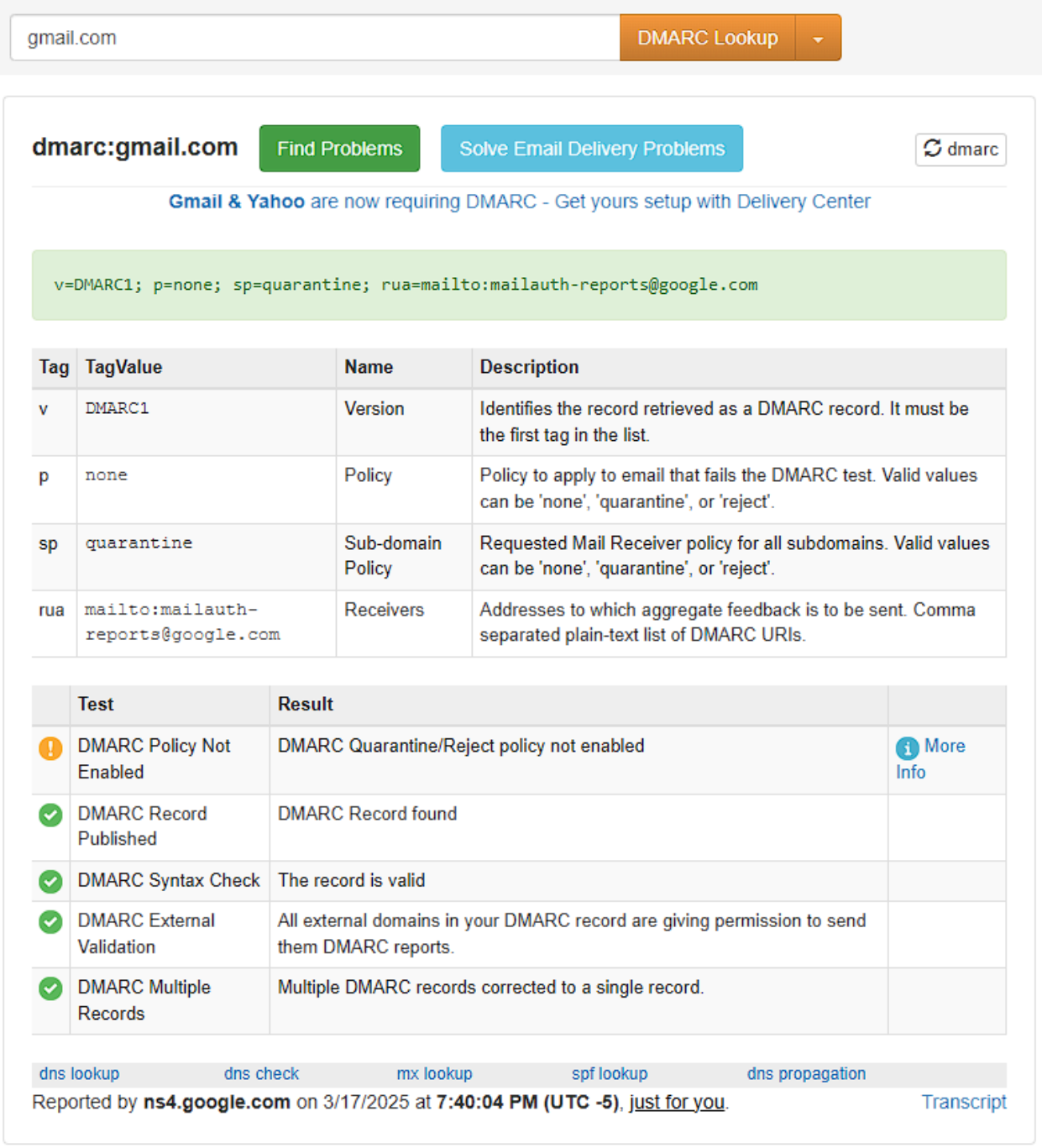
Misconfiguration in Gmail.com DMARC Policy Implementation

Summary

During our research, we identified a significant misconfiguration in Google's DMARC policy for gmail.com. This finding demonstrates that even major technology companies can make syntax errors in critical security configurations.

Technical Details

The current DMARC record for gmail.com is configured as:



This configuration contains a critical implementation error. The quarantine policy is applied to the sp tag (which only covers subdomains) rather than the p tag (which covers the main domain). With p=none, the main gmail.com domain remains unprotected by a restrictive DMARC policy.

The correct implementation should have been:

v=DMARC1; p=quarantine; sp=quarantine; rua=mailto:mailauth-reports@google.com

After careful consideration Google may have intentionally set a less restrictive DMARC policy (p=none) for the main gmail.com domain to prevent possible deliverability issues for personal Gmail users. This approach can help avoid false positives or blocks on recipient servers that are misconfigured or do not properly handle ARC (Authenticated Received Chain). By applying quarantine or more stringent rules only at the subdomain level (sp=quarantine), Gmail aims to ensure higher security for specific subdomains while minimizing the risk of legitimate user email being filtered or bounced. However, from a security standpoint, the lack of a stricter DMARC enforcement on the main domain (p=none) still represents a potential vulnerability window for spoofing, highlighting the trade-off between deliverability concerns and robust email authentication.

Impact

This misconfiguration potentially leaves the gmail.com domain more vulnerable to spoofing attacks. While Google's robust infrastructure likely provides multiple layers of security beyond DMARC, this example illustrates how syntax errors can create security gaps even in organizations with significant resources.

Recommendations

This finding emphasizes the importance of:

- Regular auditing of DNS security configurations
- Using automated validation tools to verify syntax correctness
- Implementing comprehensive testing of security policies before deployment

Wider Implications

This case demonstrates that security misconfigurations can occur in organizations of any size. If even Google can make syntax errors in security configurations, smaller organizations with fewer resources must be especially vigilant in implementing and maintaining their security policies.

NIS2 Regulation Impact

The NIS2 regulation requires registrars to implement stricter security measures, including thorough identity verification and advanced authentication, to prevent and minimize cyber incidents. These changes present technical, operational, legal, and financial challenges but also significant opportunities such as competitive advantages and increased customer trust. For domain owners, NIS2 entails stricter identity verification and strengthened authentication, along with increased protection and potential registration cost increases.

WHOIS Protocol Improvement Proposals

In light of the persistent vulnerabilities documented in this study and the reluctance of some service providers to act on critical security reports, we believe that implementing mandatory standards represents the only effective path to ensure the adoption of adequate security measures in the domain ecosystem. This section proposes an enhancement to the domain registration data access protocol through the introduction of a reliability scoring system and a "green check" to indicate a high level of security and reliability for both registrars and individual domains.

The proposal is based on integration with the Registration Data Access Protocol (RDAP), the successor to WHOIS, which offers advanced features such as authentication, authorization, and support for structured data in JSON format. By creating a system that publicly displays adherence to security standards, virtuous behaviors are incentivized even from organizations that would otherwise ignore reported vulnerabilities, as the consequences of non-compliance would become evident to both customers and business partners. The objective is to improve the security of the Internet domain ecosystem, incentivize the adoption of advanced security practices, and provide users with clear indicators of the trustworthiness of the websites they visit.

1. Introduction

The growing number of illegal and harmful online activities, often facilitated by unverified or insecure domain names, has highlighted the limitations of the current WHOIS protocol in providing reliable information on domain security. The advent of the Registration Data Access Protocol (RDAP), designed to overcome WHOIS deficiencies, offers an opportunity to improve transparency, trust, and security in the domain name ecosystem.

This proposal outlines a new approach to strengthen the security of domain registration processes through the introduction of a reliability scoring system and a green check (indicating a high level of compliance with security standards), visible in RDAP records. These new mechanisms, supported by RDAP's advanced authentication, authorization, and privacy features, aim to incentivize registrars and domain owners to adopt more robust security practices. By implementing this system, users will have clearer indicators of the reliability of the websites they visit, improving the overall security of the digital landscape.

2. Related Work

RDAP (Registration Data Access Protocol) was developed to overcome the limitations of WHOIS, introducing several advanced features:

- JSON Format: RDAP uses JSON for its responses, facilitating automated processing and integration with web and mobile applications.

- Authentication and Authorization: Supports mechanisms to control data access, essential for protecting sensitive information.

- Internationalization: Handles Unicode characters, supporting Internationalized Domain Names (IDN) and data in various languages.

- Extensibility: Allows the addition of new functionalities without compromising backward compatibility.

- Privacy Support: Enables limiting access to personal data, in compliance with data protection laws.

3. Proposal Objectives

- Improve Security: Implement a system that incentivizes the adoption of advanced security practices by registrars and domain owners.

- Increase Transparency: Provide clear and structured information on the security and reliability of domains.

- Protect Privacy: Align with data protection regulations, limiting access to unnecessary personal information.

- Facilitate Automated Processing: Use structured formats to enable integration with security applications and services.

- Incentivize Virtuous Behaviors: Reward those who achieve high security and reliability standards with a visible "green check" on the browsers.

4. Technical Specifications

4.1 Integration with RDAP

Integration Proposal:

- Extension of RDAP Schemas: Define new objects and attributes in JSON format to represent the reliability score and green check.

Example of extended RDAP response:


```
{
  "objectClassName": "domain",
  "handle": "example.tld",
  "ldhName": "example.tld",
  "reliabilityScore": 10,
  "greenCheckStatus": true,
  "greenCheckIssuer": "Registrar Accredited",
  "greenCheckIssueDate": "2023-01-01T00:00:00Z",
  "events": [
    {
      "eventAction": "registration",
      "eventDate": "2024-10-07T17:58:00Z"
    }
  ],
  "entities": [...],
  "links": [...],
  "notices": [...],
  "remarks": [...]
}
```

- Compatibility with WHOIS: Provide mapping of new fields to maintain compatibility with legacy systems.

4.2 Reliability Scoring System

The reliability scoring system evaluates both registrars and individual domains based on specific criteria. Registrars must obtain a score of 10/10 to receive the green check, while domain owners must achieve a score of 8/10.

4.2.1 Calculating the Score for Registrars

Evaluation Criteria (total 10 points):

Advanced Customer Identity Verification (2 points)

2 points: Implementation of reliable digital identification systems for complete customer identity verification, such as:

Electronic Identity Documents:

Electronic passports

Electronic identity cards

SPID (Italy) or equivalent systems in other countries

Video Call Verification: With qualified operators.

1 point: Identity verification through standard methods, such as:

Non-Electronic Identity Documents: Scanned copies of documents without in-depth electronic verification.

Email or Phone Verification: Basic contact methods.

Mandatory Two-Factor Authentication (2FA) (2 points)

2 points: Mandatory application of 2FA for access to customer control panels and registrar internal systems.

1 point: Optional 2FA application or only for some services.

Security Certifications (2 points)

2 points: Possession of internationally recognized security certifications, such as:

ISO/IEC 27001: Information security management.

ISO/IEC 27701: Privacy information management.

Other equivalent certifications.

1 point: Partial certifications or in the process of obtaining.

Adoption of SPF, DKIM, and DMARC (2 points)

2 points: Correct and active configuration of SPF, DKIM, and DMARC with restrictive policies on domains belonging to the registrar.

1 point: Partial configuration or with less restrictive policies on domains belonging to the registrar.

Documented and Published Security Policies (1 point)

1 point: Documentation and publication of internal security policies, accessible to the public or customers.

Continuous Staff Training (1 point)

1 point: Regular cybersecurity training programs for all staff, with periodic updates.

Threshold for Green Check: A score of 10/10.

4.2.2 Calculating the Score for Domains

Evaluation Criteria (total 10 points):

Owner Identity Verification (2 points)

2 points: Complete identity verification through reliable and nationally or internationally recognized methods, such as:

Electronic Identity Documents:

Electronic passports

Electronic identity cards

SPID (Italy) or equivalent systems in other countries

1 point: Complete identity verification via video call with a qualified operator.

SSL/TLS Implementation (2 points)

2 points: Use of advanced SSL/TLS certificates (OV or EV certificates) with strong encryption.

1 point: Use of valid and updated standard SSL/TLS certificates (DV).

Adoption of SPF, DKIM, and DMARC (2 points)

2 points: Correct and active configuration with restrictive policies (e.g., p=reject in DMARC).

1 point: Partial configuration or with less restrictive policies (e.g., p=quarantine in DMARC).

DNSSEC Implementation (2 points)

2 points: DNSSEC enabled and correctly configured.

1 point: DNSSEC implemented with partial or suboptimal configurations.

Absence of Malicious Activities (2 points)

2 points: The domain has not been present on any automatically consulted blacklist for at least 12 months.

1 point: The domain has not been present on any automatically consulted blacklist for at least 6 months.

Threshold for Green Check: A score of 8 or more out of 10.

4.3 Green Check for Registrars and Domains

Issuance and Verification:

- For Registrars: ICANN verifies compliance and assigns the green check.

- For Domains: The registrar verifies compliance and assigns the green check.

Display:

- In RDAP Data: Included in RDAP responses.

- For End Users: Shown in web browsers and security software.

4.4 Integration of Green Check in Web Browsers

- Display in the Address Bar

- Additional Details on Request

- Collaboration with Browser Providers

4.5 Data Security and Privacy

- Limitation of Public Data

- Access Control

- Regulatory Compliance

4.6 Use of Authentication and Authorization Mechanisms

To ensure that only authorized entities can access or modify sensitive information, such as the reliability score and green check, appropriate automated authentication mechanisms will be implemented. The implementation of these automated mechanisms is crucial to ensure that only legitimate systems and services can programmatically interact through APIs with their own data.

Authentication Mechanisms:
1. API Communication:
- Client TLS Certificates: Enabling strong mutual authentication between systems

2. Administrative Access, for human administrative access to management interfaces:
- Passkeys: Primary authentication method
- Two-Factor Authentication (2FA)
- Access logging and monitoring

4.7 Risk Management and Mitigation

- System Abuse: Use of digital signatures and certificates

- Criteria Transparency

- Continuous Monitoring

5. Implementation and Governance

5.1 Roles and Responsibilities

- ICANN: General oversight, registrar evaluation, green check assignment.

- Registrars: Implementation of security criteria, verification of client domains, assignment of green check to domains.

- Domain Owners: Adoption of necessary measures to increase reliability score.

- Browser and Security Software Providers: Integration of green check into user interfaces.

5.2 Issuance and Revocation Process

- Green Check Issuance:

  - Registrars: Assign to domains that reach the score threshold.

  - ICANN: Verifies and assigns to compliant registrars.

- Green Check Revocation: In case of non-compliance.

- Score Updates: Periodic to reflect any changes.

5.3 Transparency and Verifiability

- Public Access to Scores: Through RDAP.

- Reporting: Publication of periodic compliance reports.

- Feedback and Complaints: Mechanisms for reporting and resolution procedures.

6. Practical Considerations and Impacts

6.1 Costs and Resources

Potential Funding Sources:

- ICANN and Internal Funds
- Contributions from Registrars and Registries
- Government Grants and Public Funds
- Private Sector Partnerships
- Foundations and Non-Profit Organizations
- Innovative Funding Models

Benefits for Investors:

- Registrars and Registries: Competitive advantage, reputation improvement.
- Tech Companies and Security Providers: New business opportunities.
- Governments and Society: Improved national security, promotion of digital economy.

Strategies for Sustainable Implementation:

- Gradual Implementation Phases
- Communication and Awareness

6.2 Support for Small Registrars and Developing Countries

- Assistance Programs
- Flexibility in Implementation
- Specific Incentives

7. Implementation Plan

7.1 Roadmap

1. Development of technical specifications and evaluation criteria.
2. Consultation with stakeholders.
3. Pilot implementation.
4. Evaluation of results and modifications.
5. Global implementation.

7.2 Pilot Tests and Proof of Concept

- Objective: Evaluate effectiveness and identify issues.
- Participants: Volunteer registrars and a sample of domain owners.
- Evaluation: Feedback collection and impact measurement.

8. Stakeholder Engagement

- Registrars and Registries
- Domain Owners
- Browser Providers
- Security Organizations

9. Legal and Regulatory Considerations

- Compliance with GDPR and Other Privacy Regulations
- Data Protection

- Legal Responsibility

10. Complementary Technologies for Reliability Scoring

- DNSSEC
- SPF, DKIM, and DMARC
- Advanced SSL/TLS Certificates
- Operational Security Practices

11. Conclusions

The proposal aims to create a more secure and reliable domain ecosystem through the introduction of a reliability scoring system and a visible green check. Integration with RDAP and alignment with best practices and international standards make the proposal robust and sustainable in the long term.

Implementing this proposal will:

- Increase User Trust
- Reduce Malicious Activities
- Promote High Standards

12. References

- Technical Documents:
  - RFC 7480: HTTP Usage in RDAP
  - RFC 7481: Security Services for RDAP
  - RFC 7482: RDAP Query Format
  - RFC 7483: JSON Responses for RDAP

  - RFC 7484: Finding the Authoritative RDAP Service
- RDAP Implementations:
  - Nomulus RDAP User's Guide
- International Standards:
  - ISO/IEC 27001: Information Security Management
  - ISO/IEC 27701: Privacy Information Management
- Complementary Technologies:
  - DNSSEC: [RFC 4033, 4034, 4035]
  - SPF: [RFC 7208]
  - DKIM: [RFC 6376]
  - DMARC: [RFC 7489]
- Privacy Regulations:
  - GDPR (Europe)
  - CCPA (California)
  - LGPD (Brazil)
  - Other relevant local laws
- Organizations Involved:
  - ICANN
  - IETF
  - Web browser providers
  - RDAP communities and working groups

Note:

The future implementation of MTA-STS and DANE protocols is planned within the Reliability Scoring System criteria, aimed at further strengthening email security and protection.

Moreover, we plan to extend the Reliability Scoring System criteria to intermediaries providing email services (e.g., cloud email providers, email gateways, security filtering services), ensuring consistent security standards across the entire email delivery chain

Comparison with Other Attacks

Unlike attacks targeting technical infrastructures directly, this approach exploits weaknesses in human and administrative processes, making it particularly insidious as it bypasses many traditional technical defenses, targeting the most vulnerable point: the interface between digital systems and human processes.

Research Methodology

Our methodology combined technical analysis, ethical testing, and legal research.
We conducted tests on accounts we own with an Italian registrar, analyzed existing security policies, and studied the legal implications of current and future regulations like NIS2. This multidisciplinary approach allowed us to identify critical vulnerabilities and propose innovative solutions.

Summary

The proposed modifications to the WHOIS - RDAP protocol and the introduction of a reliability scoring system directly address the vulnerabilities identified in the Proof of Concepts (PoCs) presented earlier. Here's how each PoC is mitigated by our proposed solution:

PoC 1: Vulnerability in the Username and Password Recovery Process

- **Issues Identified**: Exploitation of non-anonymized WHOIS data and weak self-certification processes for credential recovery.
- **Proposed Solution**: Enhancing identity verification through third-party digital verification services, implementing two-factor authentication (2FA), and anonymizing WHOIS data. These measures protect domain owner information and strengthen credential recovery processes.

PoC 2: Critical Vulnerabilities in Register S.p.A Email Service

- **Issues Identified**: Poor SPF, DKIM, and DMARC configurations leading to phishing vulnerabilities.
  Poor controls on the "Use custom name" field in the webmail of *Register.it*
- **Proposed Solution**: Mandating the adoption of SPF, DKIM, and DMARC policies for registrar-managed mail servers and domains. Ensuring strict compliance with these protocols will prevent phishing attacks.
  Establish that the "Use custom name" field does not accept from user input a number of spaces greater than one.

PoC 3: Further Vulnerabilities in Register.it Email Service Allowing Phishing Attacks

- **Issues Identified**: DNS configuration issues exposing users to phishing attacks impersonating Register.it to obtain information usable in PoC 1.
- **Proposed Solution**: Advanced verification systems and continuous monitoring for registrars, along with a green check system for domains and registrars to ensure adherence to best security practices, including proper DNS configurations.

PoC 4: March 2025 Retest: Bypassing 2FA in the Credential Recovery Process (Register.it)

- **Issues Identified:** Attackers can still reset credentials and disable 2FA by submitting self-certified documents
  Only minimal additional "security notification" was added, giving domain owners insufficient time to react
- **Proposed Solutions**
  Stronger Document Verification Integrate digital ID checks or remote video verification instead of simple self-certification.
  Multi-Channel Confirmation Require multiple forms of confirmation (e.g., phone call, SMS to the original number on file) before removing 2FA.
  Real-Time Alerts Provide immediate, prominent alerts (email, SMS) to legitimate owners so they can promptly lock their account if an unauthorized reset is attempted.

PoC 5: March 2025 Retest: Persistent Email Vulnerabilities in Register.it One Year Later

- **Issues Identified:** No remediation of previously disclosed SPF/DMARC misconfigurations
  Continued ability to spoof official support emails
  Ongoing "Use custom name" exploit in webmail interface
- **Proposed Solutions**
  Urgent Policy Enforcement Adopt the same measures indicated in PoC 2 and 3 without further delays.
  Automated Monitoring Implement continuous scans that detect and flag domain-level misconfigurations.
  Revamped Webmail Security Patch the interface to disallow large whitespace usage in the sender display field.

PoC 6: Forever Day (∞-day) Vulnerability in N-ABLE Mail Assure (Affecting ~17,000 Domains)

Issues Identified

- Cross-tenant spoofing bypasses DMARC for domains sharing the same N-ABLE Mail Assure infrastructure
- Authenticated users can set MAIL FROM: any other tenant's domain

Proposed Solutions

Domain-to-Account Binding Restrict sending to only those domains explicitly owned by or delegated to the authenticated user.

Stricter SMTP Authentication Logic Enforce domain checks during the SMTP handshake, rejecting cross-tenant MAIL FROM: addresses.

Enhanced Logging & Alerting Log and alert any attempted use of unauthorized sender domains.

PoC 7: Misconfiguration in Gmail.com DMARC Policy

- **Issues Identified**

Syntax error or balance between security and usability in placing only quarantine on the sp tag instead of using p=quarantine for the main domain?

p=none weakens DMARC for gmail.com

- **Proposed Solutions**

  Syntax Corrections Update Gmail's DMARC record to v=DMARC1; p=quarantine; sp=quarantine; ...

  Regular DNS Audits Even large providers should periodically re-check DMARC, SPF, and DKIM syntax for errors.

These correlations demonstrate how the proposed RDAP improvements and reliability scoring system can effectively mitigate the vulnerabilities highlighted in our PoCs, thereby enhancing the overall security posture of domain registration and management processes.

Key Takeaways

- **Persistent Vulnerabilities:** Even critical vulnerabilities publicly disclosed often remain unresolved for extended periods, underscoring the necessity of regulatory frameworks and mandatory security standards.
- **Process Vulnerabilities:** Many significant cybersecurity risks arise from procedural weaknesses (such as credential recovery and identity verification), highlighting the need for robust digital identification and multi-factor authentication methods.
- **Standardization and Regulation:** Implementing a standardized Reliability Scoring System integrated within RDAP provides transparency, encourages proactive security adoption, and helps users easily identify trusted providers and domains.
- **Expanding Security Scope:** Future scoring enhancements, including MTA-STS and DANE, as well as extending assessments to email intermediaries, will further secure the entire communication infrastructure, not just isolated segments.
- **Continuous Improvement:** Regular auditing and timely remediation of security misconfigurations (SPF, DKIM, DMARC, DNSSEC, etc.) are vital practices, regardless of organization size or perceived security maturity.

Alessandro Bertoldi

alessandro@bertoldicybersecurity.com

linkedin.com/in/bertoldicybersecurity

bcsec.io | bertoldicybersecurity.com