PHISHING EMAIL ANALYSIS

Organization: VitalCare Health Solutions

Report: Malicious Phishing Email Analysis

Date: September 2025

Presented by:
Kiridi David Ebi

Classification: Confidential (For Internal Use Only)

Executive Summary

VitalCare Health Solutions, which supports over 500 hospitals, was targeted by a phishing campaign. Attackers posed as the security team, sending emails with a malicious link and a disguised attachment. Authentication checks: Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC), all failed. The link was tied to a malicious IP and aimed at credential theft. This aligns with MITRE ATT&CK technique T1566 (Phishing): Adversaries send deceptive emails to trick users into revealing credentials or executing malicious files

Introduction

Objective

The objective of this report is to provide VitalCare leadership with a clear, non-technical overview of the phishing attempt, its implications for the organization, and recommended actions.

Scope

The investigation focused on one phishing email sample, analyzing its sender information, content, attachments, and links. The goal was to determine risk, potential impact, and mitigation steps.

Methodology

- Reviewed email headers for authentication results (SPF, DKIM, DMARC).
- Inspected body content for social engineering cues.
- Examined attachment hash against global threat databases.
- Conducted passive checks on embedded URLs and domains.

Phishing Email Details

01 Sender: Spoofed as VitalCare Security Team

02 Subject: “Urgen: Immediate Action Required”

03 Body: Requested recipients to verify account credentials within 24 hours

04 Link: http://malicious-url.com/verify (non-secure, credential harvesting

05 Attachment: Invoice_12345.exe (malicious file disguised as invoice

06 Sender IP: 192.168.1.1 (private address, invalid for external mail

malicious-url.com

3.33.251.168 Public Scan

Lookup Go To Rescan

Add Verdict Report

URL: http://malicious-url.com/verify

Submission: On September 01 via manual (September 1st 2025, 12:53:11 am UTC) from NG — Scanned from DE

Summary | HTTP 2 | Redirects | Behaviour | Indicators | Similar | DOM | Content | API | Verdicts

2 HTTP transactions

Everything | HTML | Script | AJAX | CSS | Image | Expand all

0 data transactions

Method / Protocol	Status	Resource / Path		Size / x-fer	Time / Latency	Type / MIME-Type	IP / Location	
GET H/1.1	404 Not Found	Primary Request verify malicious-url.com/ Redirect Chain ▫ http://malicious-url.com/verify ▫ https://malicious-url.com/verify ▫ http://malicious-url.com/verify	Show response	143 B 405 B	103ms 103ms	Document text/html	3.33.251.168 AMAZON-02	
GET H/1.1	404 Not Found	favicon.ico malicious-url.com/		0 138 B	99ms 99ms	Other text/plain	3.33.251.168 AMAZON-02	

0
/ 94

Community Score 53

192.168.1.1

suspicious-udp private

Last Analys
52 minutes

DETECTION DETAILS RELATIONS COMMUNITY 282

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Whois Lookup

```
NetRange: 192.168.0.0 - 192.168.255.255
CIDR: 192.168.0.0/16
NetName: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle: NET-192-168-0-0-1
Parent: NET192 (NET-192-0-0-0-0)
NetType: IANA Special Use
Organization: Internet Assigned Numbers Authority (IANA)
RegDate: 1994-03-15
Updated: 2013-08-30
Comment: These addresses are in use by many millions of independently operated networks, which might be as small as a single computer connected to a home gatew
and are automatically configured in hundreds of millions of devices. They are only intended for use within a private context and traffic that needs to cross th
Internet will need to use a different, unique address.
Comment: These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traffic from these addresses does not come
from ICANN or IANA. We are not the source of activity you may see on logs or in e-mail records. Please refer to http://www.iana.org/abuse/answers
Comment: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC 1918 which ca
be found at:
Comment: http://datatracker.ietf.org/doc/rfc1918
Ref: https://rdap.arin.net/registry/ip/192.168.0.0
OrgName: Internet Assigned Numbers Authority
```

Indicators of Compromise (IOCs)

01 Malicious URL: http://malicious-url.com/Linked IP:15.197.225.128, 3.33.251.168

02 File attachment: Invoice_12345.exe

03 File SHA-256 hash: c27149e1cc9217925d7cd10a333408952bd3567f01e8a6ed641fc1c83053b2af

04 Spoofed domain: vitalcarehealthsolutions.com

05 Sender IP: 192.168.1.1 (invalid/private)

128

1 / 94

Community Score -9

1/94 security vendor flagged this IP address as malicious

Reanalyze Si

15.197.225.128 (15.196.0.0/14)

AS 16509 (AMAZON-02)

US

DETECTION DETAILS RELATIONS COMMUNITY 86

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you wan

Criminal IP	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean
BitDefender	Clean	Bluelix	Clean

malicious-url.com

3.33.251.168 Public Scan

Lookup Go To Rescan

Add Verdict Report

URL: http://malicious-url.com/verify

Submission: On September 01 via manual (September 1st 2025, 12:53:11 am UTC) from NG — Scanned from DE

Summary | HTTP 2 | Redirects | Behaviour | Indicators | Similar | DOM | Content | API | Verdicts

2 HTTP transactions

Everything | HTML | Script | AJAX | CSS | Image | Expand all

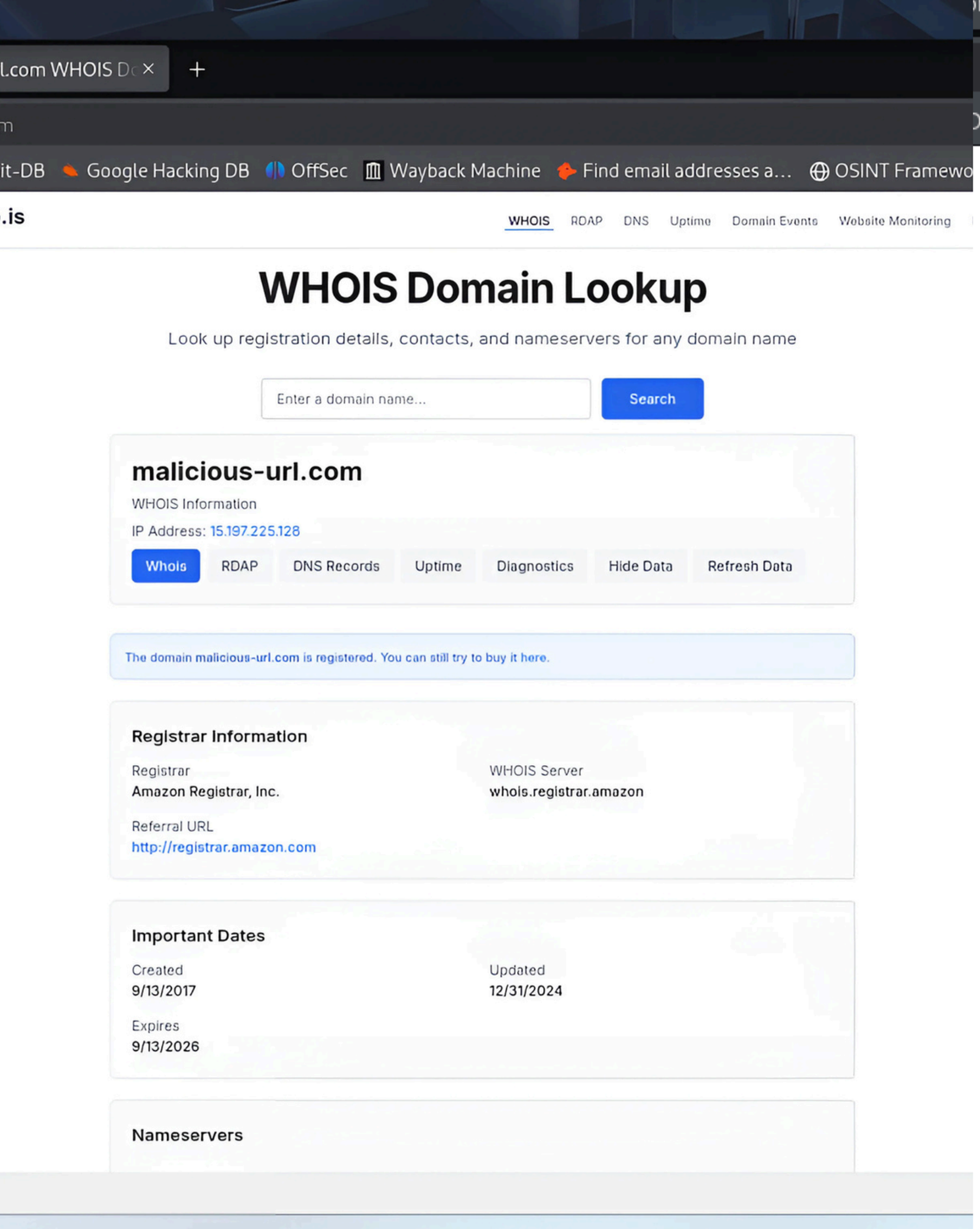
0 data transactions

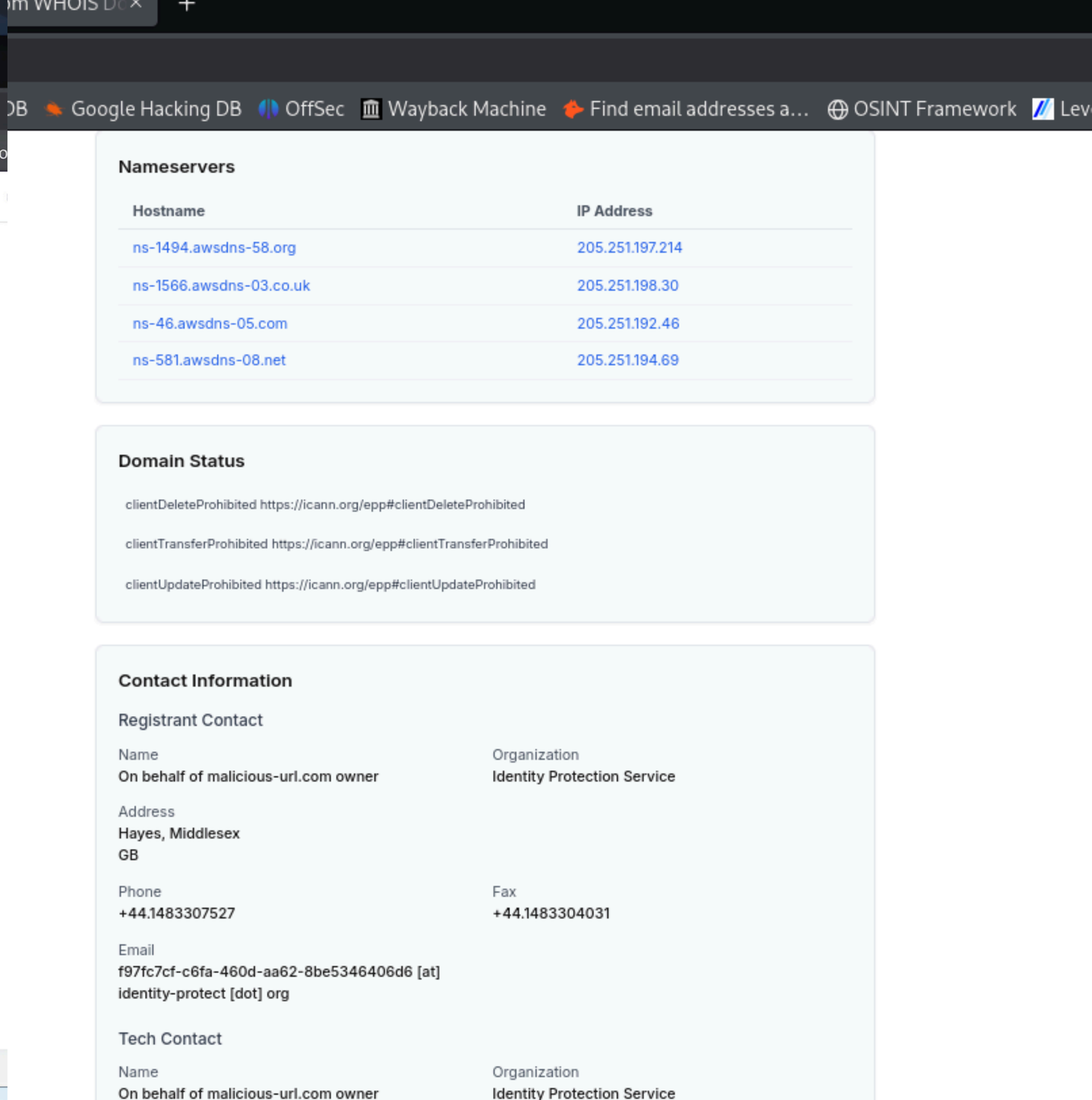
Method / Protocol	Status	Resource / Path		Size / x-fer	Time / Latency	Type / MIME-Type	IP / Location
GET H/1.1	404 Not Found	Primary Request verify malicious-url.com/ Redirect Chain: http://malicious-url.com/verify → https://malicious-url.com/verify → **http://malicious-url.com/verify**	Show response	143 B 405 B	103ms 103ms	Document text/html	3.33.251.168 AMAZON-02
GET H/1.1	404 Not Found	favicon.ico malicious-url.com/		0 138 B	99ms 99ms	Other text/plain	3.33.251.168 AMAZON-02

Analysis

The phishing email employed multiple tactics:

- Impersonation: Posed as VitalCare's own security team.
- Urgency: Pressured the recipient to act within 24 hours.
- Malicious Link: Directed victims to a fake verification page for credential theft
- Malicious Attachment: Contained an executable disguised as an invoice. VirusTotal had no prior record of this file, suggesting it was newly created to bypass defenses.
- Authentication Failure: SPF, DKIM, and DMARC all failed (see Appendix Fig. 5 – MXToolbox SPF/DMARC test).
- Malicious Infrastructure: While vendors did not flag the malicious URL, further investigation linked it to a suspicious IP (15.197.225.128), which was flagged as malicious.
- Domain Registration: WHOIS lookups revealed the domain was registered via Amazon Registrar with hidden ownership details


.com WHOIS D
it-DB
Google Hacking DB
OffSec
Wayback Machine
Find email addresses a...
OSINT Framewo
.is
WHOIS
RDAP
DNS
Uptime
Domain Events
Website Monitoring
WHOIS Domain Lookup
Look up registration details, contacts, and nameservers for any domain name
Enter a domain name...
Search
malicious-url.com
WHOIS Information
IP Address: 15.197.225.128
Whois
RDAP
DNS Records
Uptime
Diagnostics
Hide Data
Refresh Data
The domain malicious-url.com is registered. You can still try to buy it here.
Registrar Information
Registrar
Amazon Registrar, Inc.
WHOIS Server
whois.registrar.amazon
Referral URL
http://registrar.amazon.com
Important Dates
Created
9/13/2017
Updated
12/31/2024
Expires
9/13/2026
Nameservers


DB
Google Hacking DB
OffSec
Wayback Machine
Find email addresses a...
OSINT Framework
Nameservers
Hostname
IP Address
ns-1494.awsdns-58.org
205.251.197.214
ns-1566.awsdns-03.co.uk
205.251.198.30
ns-46.awsdns-05.com
205.251.192.46
ns-581.awsdns-08.net
205.251.194.69
Domain Status
clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
clientTransferProhibited https://icann.org/epp#clientTransferProhibited
clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Contact Information
Registrant Contact
Name
On behalf of malicious-url.com owner
Organization
Identity Protection Service
Address
Hayes, Middlesex
GB
Phone
+44.1483307527
Fax
+44.1483304031
Email
f97fc7cf-c6fa-460d-aa62-8be5346406d6 [at]
identity-protect [dot] org
Tech Contact
Name
On behalf of malicious-url.com owner
Organization
Identity Protection Service

Impact Assessment

Severity: High

Potential Consequences:

- Compromise of employee accounts through stolen credentials
- Malware infection from malicious attachment.
- Exposure of sensitive health data, risking HIPAA non-compliance.
- Disruption of services across VitalCare’s hospital and clinic partners.
- Reputational damage and loss of patient trust

Mitigation & Recommendations

Immediate Actions

- Block the malicious domain and hash across email, network, and endpoint systems.
- Quarantine and remove any copies of the email from user inboxes.
- Notify employees about this phishing attempt and reinforce awareness.

Long-Term Recommendations

- Strengthen DMARC enforcement to reject unauthorized mail.
- Conduct regular phishing simulations and awareness training.
- Enhance email filtering rules to flag executable attachments.
- Expand threat intelligence sharing with industry partners.

Conclusion

This phishing incident targeting VitalCare Health Solutions demonstrates the persistent and evolving threats facing healthcare organizations. The campaign was designed to bypass basic defenses and exploit human trust. By taking immediate containment steps and implementing long-term improvements, VitalCare can reduce the risk of successful attacks and continue safeguarding patient data and operational integrity.

THANK YOU FOR YOUR ATTENTION