

Abnormal

Agenda:

- **The Quishing Pipeline: Tracing the Evolution of QR Code Attacks**
- **Weaponized Evasion: CAPTCHAs, Geofencing, and Sandbox Detection Techniques**
- **Behind the Curtain: Phishing-as-a-Service (PaaS) Portal & Infrastructure Demo**

Abnormal

David Nicholson
Solutions Engineer

20 Something Years Precision Manufacturing for Defense & Healthcare

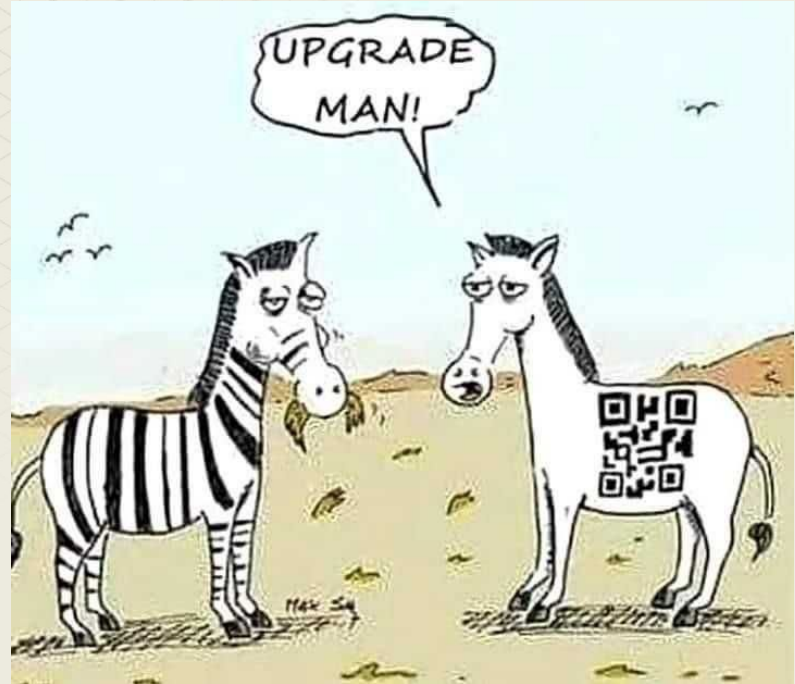
13+ Years on the vendor side:

- **9 Years @ RSA NetWitness Platform** - full packet capture, SIEM, and EDR
- **4.5 Years @ Abnormal AI:** Behavioral AI SOC Automation

10-Year DEF CON Attendee | 3-Year RSAC SOC & DEF CON NOC Analyst

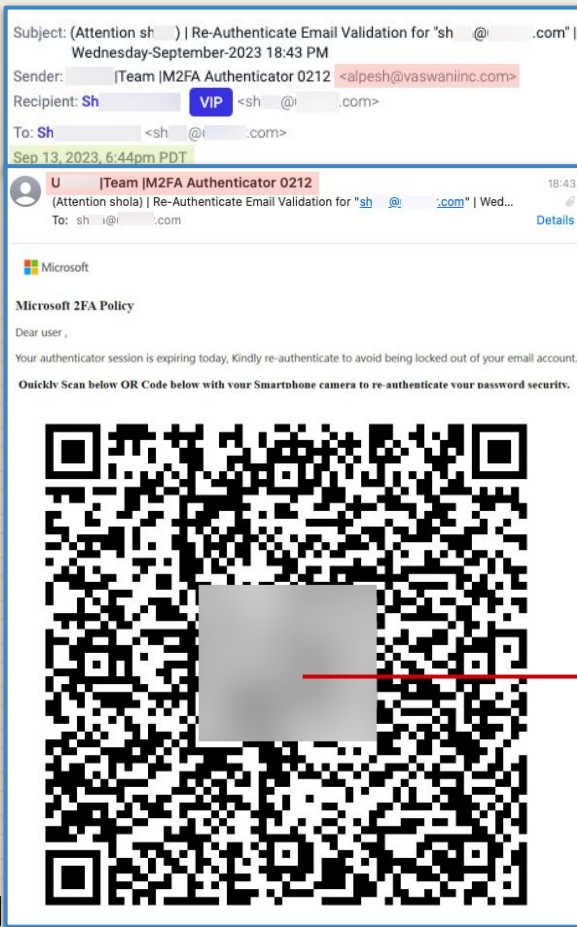
Abnormal

Evolution of QR Code Attacks



Anonymized Attack Case

QR Code Image - IT Impersonation

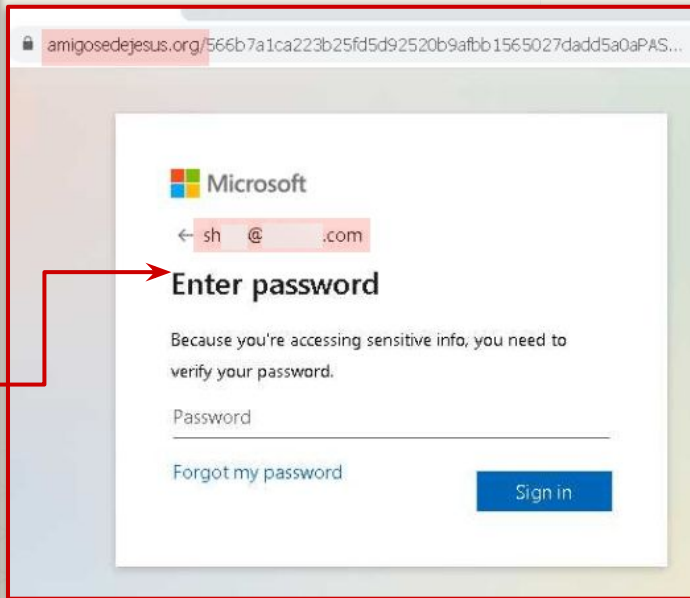
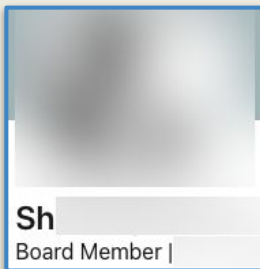


Sender Authentication

SPF: **NONE**

DKIM: **NONE**

DMARC: **NONE**



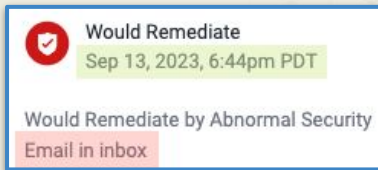
Attack Breakdown

Payload

- Message body is an image
- Link embedded in QR Code

Technique

- Phishing attack impersonating IT/Microsoft Authentication
- Deceive end users who frequently open and click links for this type of message
- Encode malicious link in QR code to obfuscate it from security controls



QR Code Image - DocuSign Impersonation

Subject: Brokerage Final Review: - Complete Document Distribution:Sign&Retur...
Sender: Brokerage@Scanner Notification <admin@hexaquestglobal.com>
Recipient: Gina <Gina@brokerage.net>
To: Gina <Gina@brokerage.net>
Oct 16, 2023, 10:21am PDT

CN Brokerage@Scanner Notification <admin@hexaquestglobal.com> 10:21
Brokerage Final Review: - Complete Document Distribution:Sign&Retur...
To: gina@brokerage.net Details

Received (2) Forwarded Replied

Recipient	Email Label/Location
Gina <Gina@brokerage.net>	deletedItems
Kaye <Kaye@brokerage.net>	inbox

Type	Source	Link URL
Qr code	Attachment	https://www.bing.com/ck/a?!I&p=b69e89ba3d924885JmldtHM9MTY5NjU1MDQwMCZpZ3VpZD0yNDFINDecyNC0xZjAwLTZlYTYtMTJlZS01NDBhMWWiZTZmMUYmaW5zaWQ9NTE3NA&ptn=3&hsh=3&fclid=241b4724-1f00-6ea6-12be-540a1ebe6f1f&u=a1aHR0cHM6Ly9waW5qYW1hbm9ubGluZS5vcmcvbGFtYW4tY29uZG9oLw#M=gina@brokerage.net

DocuSign

You have received a new document to review and sign

To review, scan the QR code above.

All parties have completed Complete with DocuSign: doc20230516211407.pdf.

Do Not Share This Email
This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.

IEFHVAKVMC.JPG

MD5 5bf0121ba0bef865f4a978bdb4533941

SHA256 78ee4b4fe917c83a660512d04351354d5c5373ac0d8f27a80b7de34d43bb81b4

Type JPG

Size 44.73KB

File Text Analysis

Anchor text phrases (message, document, password) Anchor text phrases (privacy, terms of service, unsubscribe)

Anchor text phrases (view, click, download) Credential fraud text Document sharing text

Election interference vocabulary Email admin display name impersonation Financial text Personal information

Attack Breakdown

Payload

- Body of message is an image

Technique

- Deceive end users who trust the brand and frequently open and click links in these messages
- DocuSign branding
- Link with redirect encoded in QR code
- Redirect to credential phishing site hosted with Cloudflare

 Would Remediate
Oct 16, 2023, 10:21am PDT

Would Remediate by Abnormal Security

QR Code Delivery Continued to Evolve

Protect your organizations against QR code phishing with Defender for Office 365



UrjaGandhi  MICROSOFT

Dec 12, 2023

QR code phishing campaigns have most recently become the fastest growing type of email-based attack. These types of attacks are growing and embed QR code images linked to malicious content directly into the email body, to evade detection. They often entice unwitting users with seemingly genuine prompts, like a password reset or a two-factor authentication request. [Microsoft Defender for Office 365](#) is continuously adapting as threat actors evolve their methodologies. In this blog post we'll share more details on how we're helping defenders address this threat and keeping end-users safe.

QR Code Protection

Details

- In 2023, QR codes exploded in popularity and gateways/Microsoft released capabilities to provide better protection against QR codes.
- This mainly helped with QR codes delivered via .PNGs but attackers continued to innovate on how those attacks were delivered.

QR Code embedded in PDF - HR Impersonation

Subject: Please Review Adjusted Payroll Changes 12/08 Adjustment Claim#9

Sender: HR <sales@mductsfabrication.in>

Recipient: Moe VIP <BMoe.org>

Aug 12, 2024, 5:04am PDT

EXTERNAL EMAIL: This email originated from outside of . Do not click links or open attachments unless you recognize the sender and know the content is safe.

Please find the attached HR Employee Manual (PDF). If you have any questions, don't hesitate to reach out. Sent from my iPhone.



Human Resources Training and Awareness Handbook

Volume 1
Copyright 2024 cvsonline

An employee handbook is a manual that help HR teams communicate what's expected from employees and what is undesirable it acts as a reference guide that helps align employees with the company's values, policies, and procedures.

Employee should be aware of this Cyber security awareness:
Malicious Content Download: Never click on suspicious links or Suspicious attachments.
Always report suspicious activity

Employee may also notice new premium deduction plan under "Section 125" of the IRS Code. This allows you to take advantage of federal and state laws. Contact HR "HumanResources@" for a waiver form if you elect to pay for your benefits with after-tax dollars.



Submit and complete orders, upon receipt from agencies, immediately to avoid disciplinary or possible delays with upcoming payroll processing's. Navigate to the HR Secure Barcode portal Above to Acknowledge the review of the HR awareness relational Development.

CONFIDENTIALITY NOTICE: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential information and privileged information. Any unauthorized retention, review, printing, copying, disclosure or distribution is prohibited. If you are not one of the intended recipients, please contact the sender by reply email or phone, destroy all copies of the original message and keep the information contained here confidential.

Sender Authentication

SPF: PASS

DKIM: NONE

DMARC: NEUTRAL

UNCOMMON ATTACHMENT TYPE

We have rarely seen sender domain mductsfabrication.in send emails containing attachments with extensions: pdf.

Payroll-Deductions Adjustment-65196.pdf

MD5 bbb9bcd599feecfdc72b64f37297525

SHA256 793552fe6dab8b3df0408e4c8f31f6d21485c0640f842139b47992d435d84020

Type PDF ! Uncommon Attachment Type

Size 113.28KB

File Text

Analysis

Anchor text phrases (message, document, password)

Anchor text phrases (privacy, terms of service, unsubscribe)

Anchor text phrases (view, click, download) Document sharing text

Election interference vocabulary Email admin display name impersonation

Financial intent text Financial text Payroll text Personal information

Phone scam vocabulary Releasing payment request vocabulary Urgent text

Type	Source	Link URL
QR code	Attachment	https://abaconnct.com/?ofcpkzyj

Domain:	abaconnct.com
Registrar:	NameCheap, Inc
Registered On:	2024-04-24

Attack Breakdown

Payload

- QR Code embedded in PDF

Technique

- Deceive end users who trust the brand and frequently open and click links in these messages
- Phishing attack impersonating HR Team
- QR codes obfuscate malicious links from detection tools

Would Remediate

Aug 12, 2024, 5:05am PDT

Would Remediate by Abnormal Security

Email in inbox

QR Code Generated by Google API - IT Impersonation

Subject: e-Secure Notice!!! 11/6/2023

Sender: [redacted] e-Secure Admin <jonas.niggemann@ki.tng.de>

Recipient: Bonnie [redacted] VIP <Bonnie.[redacted]@[redacted].com>

To: Bonnie [redacted] <Bonnie.[redacted]@[redacted].com>

Nov 6, 2023, 3:12am PST

SA [redacted] e-Secure Admin November 6, 2023 at 03:12
e-Secure Notice!!!! 11/6/2023
To: bonnie [redacted] j@[redacted].com

You don't often get email from jonas.niggemann@ki.tng.de. [Learn why this is important](#)



e-Secure 11/6/2023.
2FA* [redacted].com *Update*

Your bonnie [redacted]@ [redacted].com access was updated on Monday, November 6, 2023.

Scan the QR image below with your smartphone camera to complete security update.

Click "[Show blocked content](#)" to display QR image.



e-Secure

The information contained in this email is intended only for the person or entity to whom it is addressed and may contain confidential or privileged material; unauthorized use of this information is prohibited. If you have received this in error, please notify the sender and delete the material immediately. -- Thank you.

Sender Authentication

SPF: PASS

DKIM: PASS

DMARC: NEUTRAL

BK Bonnie [redacted] VIP

bonnie.[redacted]@[redacted].com

Title Vice President

Manager  Russ [redacted]

Received (2) Forwarded Replied

Recipient

Bill [redacted] VIP
Bill.[redacted]@[redacted].com

Bonnie [redacted] VIP
Bonnie.[redacted]@[redacted].com

[https://chart.apis.google\[.\]com/chart?chs=210x210&cht=qr&chld=L&chl=https://pub-62d74be2265b4451977f8c5ab7a46f21.r2\[.\]dev/z1.html?z1=Ym9ubm.....](https://chart.apis.google[.]com/chart?chs=210x210&cht=qr&chld=L&chl=https://pub-62d74be2265b4451977f8c5ab7a46f21.r2[.]dev/z1.html?z1=Ym9ubm.....)

Input

Ym9ubmllLmtoY

Output

bonnie.[redacted]@[redacted].com

<https://pub-62d74be2265b4451977f8c5ab7a46f21.r2.dev/Upload.html#bonnie>

← bonnie [redacted]@

Enter password

Password

[Forgot my password](#)

Sign in

Attack Breakdown

IT Impersonation

Payload

- Link to credential phishing site
- QR Code generated on the fly

Technique

- Deceive end users who frequently open and click links for this type of message
- Phishing attack impersonating IT/Microsoft and delivering attack
- Use of googles chart api to adhoc generate a QR code

QR Code Phishing via Corrupted .docx

Subject: Amendment for [REDACTED] Check out your Benefit/Bonus for [REDACTED] Activities for the 4th Quarter (SEP-DEC 2024)- lyNURVhUTIVNUKFORE9NNzUjlw==

Sender: HR Admin/Group Payroll [REDACTED] lyNURVhUTIVNUKFORE9NMTAwlyM= <sato.kaede@garde-intl.com>

Recipient: Judy [REDACTED]

To: Judy [REDACTED]

Nov 19, 2024, 3:17pm MST



Q4_Benefits_& Bon...
87.6 KB

Download

Preview

This message is high priority.



Microsoft Word

Word found unreadable content in Q4_Benefits_& Bonus_for_[REDACTED]#lyNURVhUTIVNUKFORE9NNDUjlw==..... Do you want to recover the contents of this document? If you trust the source of this document, click Yes.

No

Yes

[REDACTED] Benefits/Salary & Bonus Adjustment

Access your secure document by scanning the QR code below with your smartphone. This will take you directly to the document review page.



Disclaimer: This communication, including any attachments, is confidential and may be legally privileged. If you are not the intended recipient, please notify the sender and delete this communication immediately. We are not responsible for any damage caused by viruses.

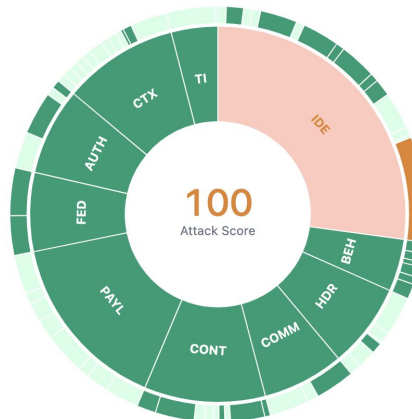


Would Remediate

Nov 19, 2024, 3:17pm MST

Would Remediate by Abnormal Security

Analysis Overview ⓘ



Abnormal Security has flagged this as a possible **Credential Phishing**.

UNCOMMON ATTACHMENT TYPE

We have rarely seen sender domain garde-intl.com send emails containing attachments with extensions: docx.

UNUSUAL SENDER

The email exhibits suspicious sending behavior: Abnormal Security has rarely ever seen the email address sato.kaede@garde-intl.com sending to your organization.

Attack Breakdown

Payload

- Targeted phishing attack that aims to compromise credentials
- Leverages corrupted .docx to bypass sandbox approach of MSFT
- <https://www.bleepingcomputer.com/news/security/novel-phishing-campaign-uses-corrupted-word-documents-to-evade-security/>

QR Code in PDF with anchor to DocuSign

BB Bobby
- Christmas bonus -***Additional payroll and ben...
To: bobby@...@...

Sender Display Name
bobby brown
UNUSUAL SENDER DOMAIN
Sender Email Address
hotelceibodorado@hotelceibodorado.com.ec
UNKNOWN IDENTITY

LINK(S) DETECTED IN ATTACHMENT
The email attachment contains a url link to an external website.

Type	Source	Link URL
QR code	Attachment	http://dhzyxo.promptexpression.com/?e=Ym9iYnkuY
QR code	Attachment	https://eu.docusign.net/Member/EmailStart.aspx?a=0f4a0415-9abb-4b04-bc4b-5544275b012d&acct=aee7f4d-70d4-4d42-89ef-0306ed9abffe&er=8107520c-6b9b-4020-a555-599db953348b

DocuSign Link is embedded using PDF annotation.

Additional_Payroll_and_Benefit_Sheet_ChristmasBenefitDetails_127855865 -
Ym9iYnkuYnJvd25AZHJ1dmEuY29tCPSSFk- Bonus Team5865337262 tmaogcdstd.pdf

MD5 4e06067b5ae237e6e61f0e583dd0663f
SHA256 6b33f8b3e3e9efb030b6ce1d4c97203706134a20cc05ef2d5ff3dfe792f56c7e

Type PDF
Size 39.75KB
File Text Analysis
Anchor text phrases (message, document, password)
Anchor text phrases (view, click, download) Credential fraud text Document sharing text
Email admin display name impersonation Financial intent text Financial text Payroll text
Phone number Releasing payment request vocabulary

! Uncommon Attachment Type

Attack Breakdown

Payload

- PDF with embedded QR Code

Technique

- Use sources like LinkedIn to determine who to target
- Deceive end users who trust the brand and frequently open and click links in these messages
- PDF QR code with malicious destination
- PDF has a second link in the corner of the QR code using PDF annotation

Input

Ym9iYnkuY

Output

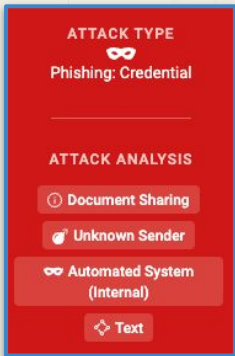
bobby. @. com



Would Remediate

Dec 18, 2024, 8:46am PST

Would Remediate by Abnormal Security



Payload

- No Attachments
- Link to Logo
- QR Code is comprised of text

Technique

- Deceive end users who trust the brand and frequently open and click links in these messages
- Phishing attack impersonating Docusign
- QR codes obfuscate malicious links from detection tools
- Imageless QR code comprised of text



<https://github.com/Flangvik/QRucible>

Abnormal Offerings



Inbound Email Security

Inbound Email Attack Protection



- Business Email Compromise (BEC)
- Supply Chain Compromise
- Invoice and Payment Fraud
- Spam
- Malware and Ransomware
- Lateral Attacks
- Credential Phishing

Remediation

- Custom AI Models
- AI-Automated Remediation
- Suspicious URL Rewriting
- Optional, fine-grained control and blocking

Platform Capabilities

Visibility

- Threat Log
- User and Activity Monitoring
- AI Data Analyst
- Notifications and Alerts
- Business Value Dashboard

SOC Productivity

- Search and Respond
- Detection 360
- Threat Log
- Quarantine Release for Microsoft

Integrations

- AI App Store
- SIEM/SOAR/EDR /XDR
- IDP
- REST API

Controls

- Global Safelist and Blocklist
- RBAC
- Audit Log

Behavioral Intelligence

- Applications
- Human Identities
- Tenants
- Supply Chain
- Threats

+ Email Security

AI Security Mailbox

Completely automate your user-reported email workflow.

- Automated Triage and Response
- Centralized Visibility and Reporting
- Personalized AI Responses to Users



Email Productivity

Improve employee productivity with adaptive graymail protection.

- Grayscale Detection and Remediation
- End-User Personalization
- Productivity Insights



Misdirected Email Prevention

Prevent data leaks caused by emails sent to incorrect recipients.

- AI Detection
- Automatic Quarantine
- End-User Remediation



AI Phishing Coach

Reduce phishing susceptibility with in-the-moment, personalized security training.

- Personalized Simulations
- Just-in-Time Training
- Training Video Content



Account Takeover Protection

Uniformly monitor and analyze every human across the cloud environment with autonomous AI.

- Continuous AI Detection
- Behavioral Case Timeline
- Real-Time Disarming



Security Posture Management

Discover and mitigate misconfiguration risk across your cloud email.

- AI-Driven Benchmark Scores
- Drift Alerts
- Actionable Remediation



Messaging Security

Secure communications platforms using behavior AI to identify anomalous activity.

- URL and Attachment Protection
- AI-Automated Remediation
- Unified Email and Message Threat Response



+ Identity Security, AI Security, and Insider Threat

Identity Threat Protection

Use behavioral AI to prevent newsworthy identity breaches.

- Threat Library, Detection, and Response
- Identity Security Posture Management
- Adaptive Identity Reset



AI Governance

Secure AI transformation through automated discovery, risk scoring, and governance.

- AI Tool Discovery
- Agent and Chat Visibility
- Automated Enforcement



Infiltration Prevention

Stop malicious actors using fabricated identities before they ever get provisioned.

- Behavioral Fraud Detection
- Cross-Org Campaign Identification
- Automated Evidence Enrichment



Abnormal

Thank You