Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

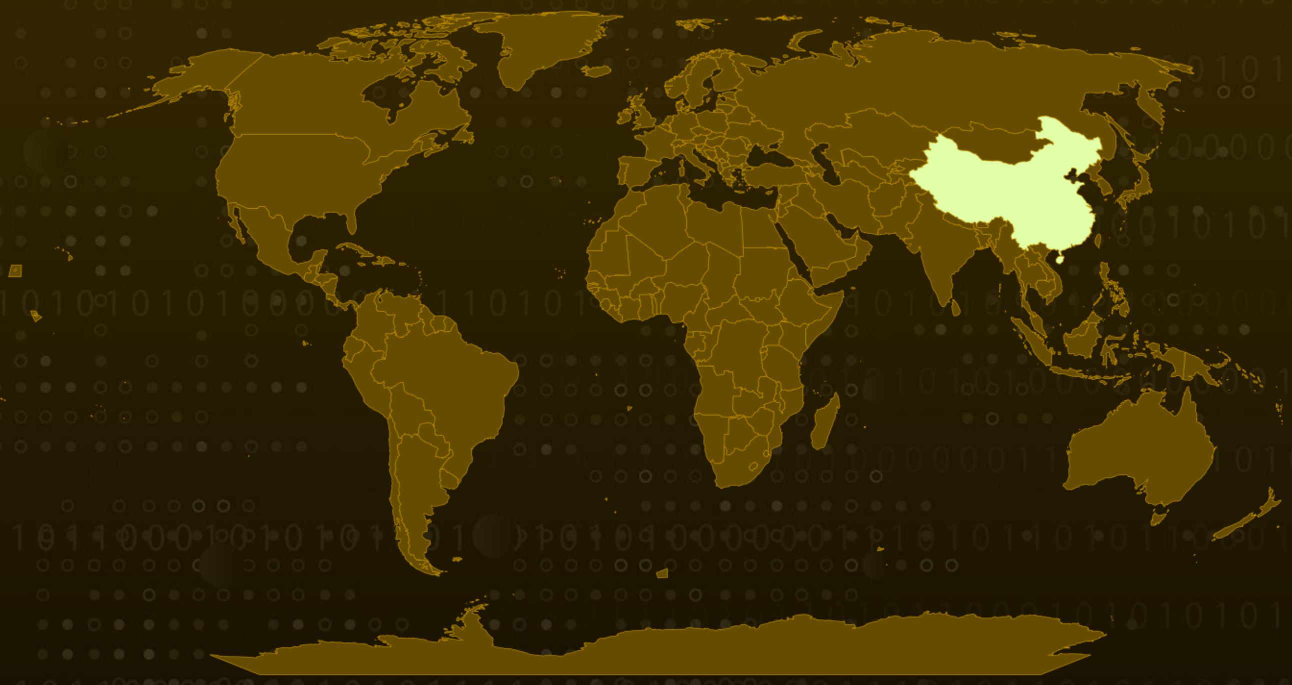
Surge in QR Code Phishing Attacks, Hits Chinese Citizens

Date of Publication	Admiralty Code	TA Number
June 20, 2024	A1	TA2024236

Summary

Attack Discovered: 2024
Attack Region: China
Attack: A new attack vector has emerged, exploiting QR codes to lure users into phishing traps. A recent campaign targeting individuals in China is using Microsoft Word documents for QR code-based phishing attacks. These files, suspected to be distributed via spam email attachments, masquerade as official documents from the Ministry of Human Resources and Social Security of China.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 QR codes have become a favored tool for cybercriminals to lure users into phishing traps. In 2024, there's been a 22% increase in QR code phishing attacks, with 89.3% of these aiming to steal credentials. The challenge lies in QR codes obscuring the actual website URL, making it tough for users to verify if it's safe.

#2 Recently, a troubling campaign was uncovered using Microsoft Word documents in QR code phishing attacks targeted at people in China. These deceptive documents, likely distributed through spam email attachments, masquerade as notices offering labor subsidies from a Chinese government agency. They trick users into scanning a QR code under the guise of applying for these subsidies.

#3 When someone scans the QR code embedded in the Word document, they're redirected to a website with the subdomain "tiozl[.]cn," hosted on IP address "20.2.161[.]134". This domain is linked to five other domains, including four subdomains of "tiozl[.]cn" and one of "zcyyl[.]com". All of these domains are part of the same large-scale phishing campaign.

#4 On the landing page, users are promised a labor subsidy and asked to input personal details like their name and national ID. The site then requests sensitive financial information such as bank card details, phone number, and current balance. To further deceive, users are prompted to enter their bank card password and withdrawal password, which are often the same as those used for domestic transactions.

#5 Unfortunately, this information isn't used for legitimate purposes. Instead, it's collected by cybercriminals to carry out unauthorized transactions, potentially causing significant financial harm to victims.

#6 This surge in QR code phishing attacks underscores how cybercriminals are becoming more sophisticated and adaptable. The targeted campaign in China highlights the serious risk posed by these tactics. It's crucial for everyone to remain vigilant and ensure robust security measures are in place to protect against such threats. Always verify the legitimacy of QR codes before scanning, especially when they're embedded in unexpected or unsolicited documents or emails.

Recommendations

Exercise Caution with Unsolicited Emails: Always exercise caution when receiving unexpected or urgent emails, especially those from unknown sources. Avoid downloading attachments from unsolicited emails to mitigate the risk of malware infections.

URL Inspection: Check the URL carefully after scanning a QR code before continuing. Keep an eye out for official domains and secure connections (https://) as indicators of validity.

Multi-Factor Authentication (MFA): Implement multi-factor authentication across all user accounts to strengthen access controls. This additional layer of security reduces the risk of unauthorized access, even if passwords are compromised.

Verify the source before scanning QR codes: Exercise caution when encountering QR codes in unsolicited emails, text messages, or documents, especially those offering money, prizes, or requiring immediate action.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0009 Collection	TA0040 Impact	T1566 Phishing	T1566.001 Spearphishing Attachment
T1204 User Execution	T1204.001 Malicious Link	T1036 Masquerading	T1657 Financial Theft
T1598 Phishing for Information			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	8462bae8b5ac446fefab66d036696d4c29648052c35edb1ba7057e39808803fa, 0dd2010270a61fd09b185e8116857d0ff36ce1a22f25d6cb1f0ddb09fa375511, e6f3c3b292e0b28e607131195edbaa00235dd555b4e5d1d7ca44e0d5975c111e, b2cb6383ee2e192f3d6adfdab367d876506aa736556dcda5d46257a2801e508c, 8551dfdc9dc899815155403d05664eea34e7e4edc950292ee5e7a4edc0a277e9, 47ffcfaf7126e90c7abbae83f7e572607df79477a24103ef8ec7aea75f52cb25, 6b7bb24281f720c16f626103f019882ca6144a2dc87f83df605861bc59ee6b14, d0a216f854b6849189b66efe7248a27d4ad5a8ae89a838d873392db42964b595
URL	hxxp://wj[.]zhvsp[.]com, hxxp://ks[.]ozzlds[.]com, hxxp://rc[.]nggznm[.]cn, hxxp://ry[.]ngghznm[.]cn, hxxp://web[.]ioomk-1[.]sbs
Domains	2wxlrl[.]tiozl[.]cn, op18bw[.]tiozl[.]cn, gzha31[.]tiozl[.]cn, i5xydb[.]tiozl[.]cn, hzrz7c[.]zcyyl[.]com, web[.]innki-1[.]sbs, web[.]oiiunm-4[.]sbs, web[.]liooik-2[.]sbs, web[.]jneuz-4[.]sbs, web[.]yoopk-4[.]sbs, web[.]ioomil-4[.]cfd, web[.]miiokn-4[.]sbs, wweb[.]muuikj-6[.]sbs, web[.]ikubzn9-1[.]sbs, inb[.]yhuiz-5[.]sbs, admin[.]yhuiz-4[.]sbs, web[.]otuz1-2[.]sbs, fmqe9s[.]jikknzjd.cn, wqegi8[.]skqkkdm[.]cn, nhfvhi[.]skqkkdm[.]cn,

TYPE	VALUE
Domains	k7pnec[.]skqkkdm[.]cn, qerxjj[.]uehsht[.]cn, vjym48[.]uehsht[.]cn, y1hc3j[.]rygwnr[.]cn, ofwdfq[.]qttsgzhcn[.]cn, g97hwf[.]okdmzjcm[.]cn, thrrai.okdmzjcm[.]cn, f8lhst[.]okdmzjcm.cn, xzlky6[.]uhhsjzn[.]cn, rcgali[.]uhhsjzn[.]cn, azure[.]5atrade[.]cf, ahgfus[.]pixqd[.]cn, sfdncx[.]lppdzna[.]cn, cjpb1j[.]lppdzna[.]cn, cqy8ek[.]poozpd[.]cn, fyo63q[.]wiiaks[.]cn, l9qxrr[.]wiiaks[.]cn, yzfpmj[.]wiiaks[.]cn, zcqgtm[.]wiiaks[.]cn, inwp8n[.]ekksjcm[.]cn, xicfpx[.]ekksjcm[.]cn

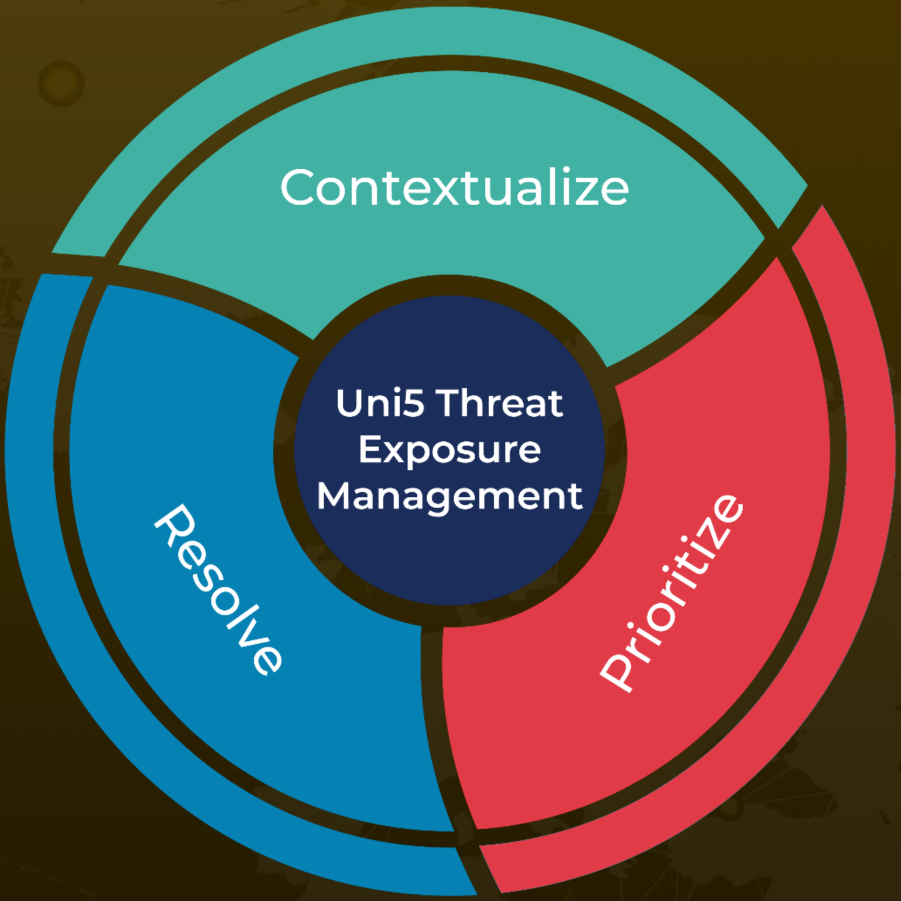
References

https://cyble.com/blog/rising-wave-of-qr-code-phishing-attacks-chinese-citizens-targeted-using-fake-official-documents/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 20, 2024 • 5:30 AM

More at www.hivepro.com