# Fighting an emerging cybercrime trend

blogs.microsoft.com/on-the-issues/2021/07/19/cybercrime-homoglyphs-dcu-court-order/

July 19, 2021

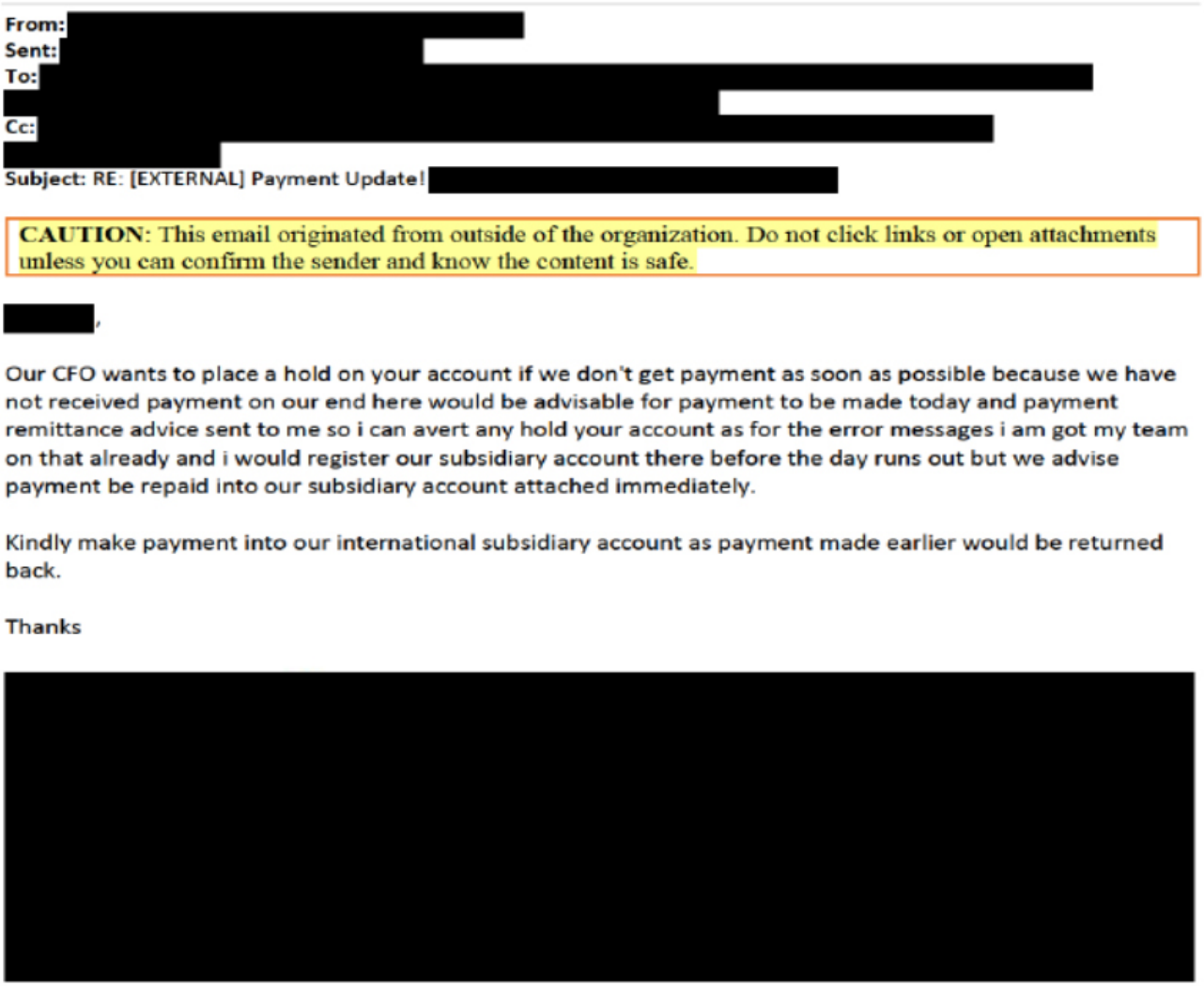
On July 16, Microsoft's Digital Crimes Unit (DCU) again secured a court order to take down malicious infrastructure used by cybercriminals. As we continually explore new ways to combat emerging trends and techniques to better protect our customers, we filed this case to target the use of "homoglyph" – or imposter – domains that are increasingly being used in a variety of attacks. As a result, a judge in the Eastern District of Virginia issued a court order requiring domain registrars to disable service on malicious domains that have been used to impersonate Microsoft customers and commit fraud.

These malicious homoglyphs exploit similarities of alpha-numeric characters to create deceptive domains to unlawfully impersonate legitimate organizations. For example, a homoglyph domain may utilize characters with shapes that appear identical or very similar to the characters of a legitimate domain, such as the capital letter "O" and the number "0" (e.g. MICROSOFT.COM vs. MICR0S0FT.COM) or an uppercase "I" and a lowercase "l" (e.g. MICROSOFT.COM vs. MICROSOFT.COM). We continue to see this technique used in business email compromise (BEC), nation state activity, malware and ransomware distribution, often combined with credential phishing and account compromise to deceive victims and infiltrate customer networks.

This case started with a single customer complaint regarding BEC, and our investigation revealed that this criminal group had created 17 additional malicious homoglyph domains that were registered with third parties. The targets are predominantly small businesses operating in North America across several industries. Based on the techniques deployed, the criminals appear to be financially motivated, and we believe they are part of an extensive network that appears to be based out of West Africa.

In this BEC attack, these fraudulent domains, together with stolen customer credentials, were used by cybercriminals to unlawfully access and monitor accounts. The group proceeded to gather intelligence to impersonate these customers in an attempt to trick victims into transferring funds to the cybercriminals. Once the criminals gained access to a network, they imitated customer employees and targeted their trusted networks, vendors, contractors and agents in an effort to deceive them into sending or approving fraudulent financial payments.

In this instance, the criminals identified a legitimate email communication from the compromised account of an Office 365 customer referencing payment issues and asking for advice on processing payments. The criminals capitalized on this information and sent an impersonation email from a homoglyph domain using the *same sender name* and *nearly identical domain*. The only difference between the genuine communication and the imposter communication was a single letter changed in the mail exchange domain, done to escape notice of the recipient and deceive them into believing the email was a legitimate communication from a known trusted source. As seen in the example below, these criminals used the same subject line and format of an email from the earlier, legitimate conversation, but falsely claimed a hold had been placed on the account by the CFO, time was running out and payment needed to be received as soon as possible.



From: [redacted]
Sent: [redacted]
To: [redacted]
Cc: [redacted]
Subject: RE: [EXTERNAL] Payment Update! [redacted]

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you can confirm the sender and know the content is safe.

[redacted],

Our CFO wants to place a hold on your account if we don't get payment as soon as possible because we have not received payment on our end here would be advisable for payment to be made today and payment remittance advice sent to me so i can avert any hold your account as for the error messages i am got my team on that already and i would register our subsidiary account there before the day runs out but we advise payment be repaid into our subsidiary account attached immediately.

Kindly make payment into our international subsidiary account as payment made earlier would be returned back.

Thanks

[redacted]

Often, once detected or addressed by Microsoft through technical means, these criminals move their malicious infrastructure outside the Microsoft ecosystem and onto third-party services in an attempt to continue their illegal activities. With this case, we secured an order which eliminates the defendants' ability to move these domains to other providers. The action will further allow us to diminish the criminals' capabilities and, more importantly, obtain additional evidence to undertake further disruptions inside and outside court. This disruption effort follows 23 previous legal actions against malware and nation-state groups that we've taken in collaboration with law enforcement and other partners since 2010.

Microsoft goes to great lengths to protect customer accounts. Office 365 uses real-time anti-spam and multiple anti-malware engines to prevent threats from reaching their inboxes. Microsoft also offers Defender for Office 365, which helps protect customers against new, sophisticated attacks in real time. When we identify customer accounts that have been targeted or compromised, such as the ones in today's court order, or where our investigations uncover homoglyph domains impersonating customers, we provide notice through the Microsoft 365 Message Center.

Cybercriminals are getting more sophisticated. Microsoft's Digital Crimes Unit will continue to fight cybercrime with our comprehensive efforts to disrupt the malicious infrastructure used by criminals, through referrals to law enforcement, civil legal actions on behalf of our customers such as this one, or technical measures in partnership with our product and service teams. Organizations should regularly check for messages in the Microsoft 365 Message Center and can follow these steps to prevent BEC attacks.

Tags: business email compromise, cybersecurity, Digital Crimes Unit, homoglyphs, malware, phishing