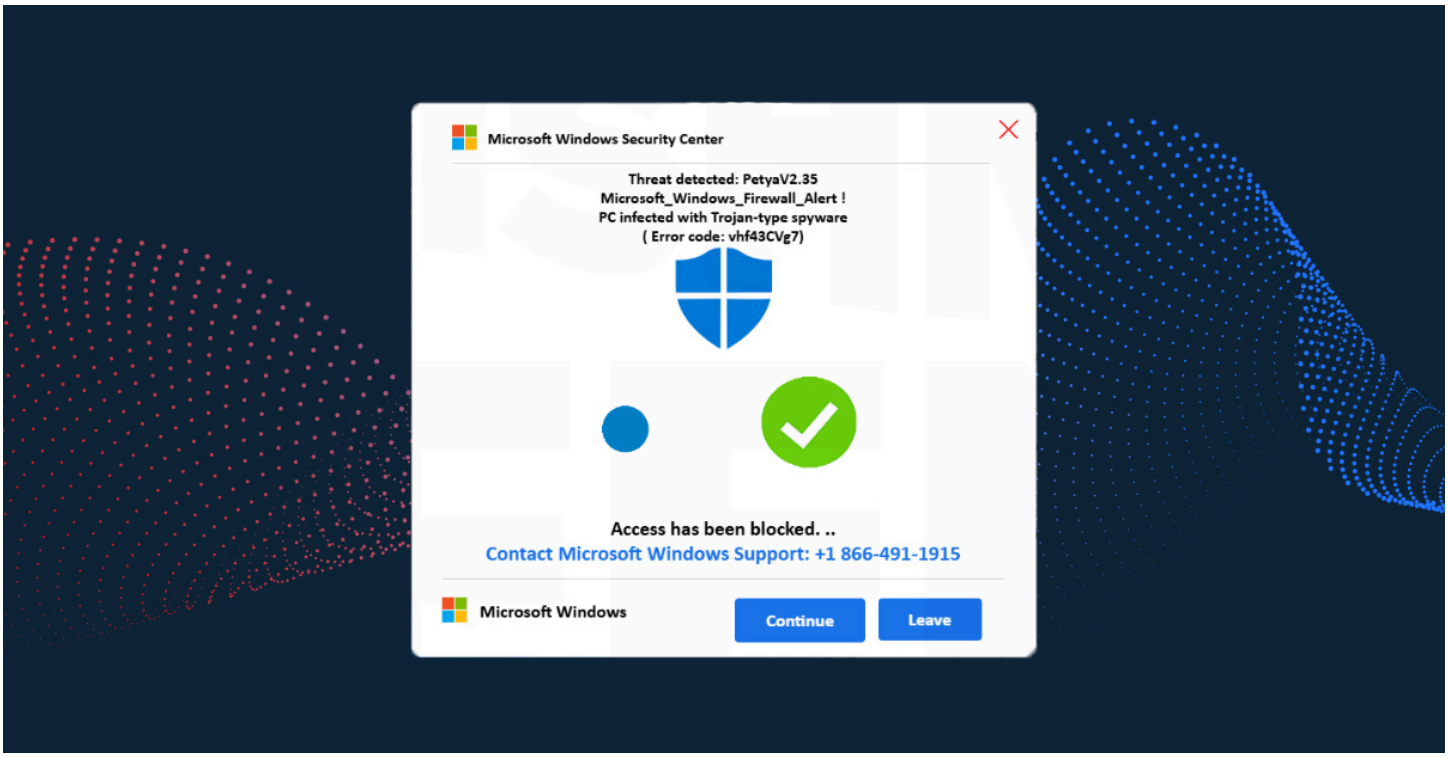
Weaponized Trust: Microsoft's Logo as a Gateway to Tech Support Scams



By: Dylan Main, Cofense Phishing Defense Center

The brand name Microsoft has been ingrained in our vocabulary for nearly half a century. It is a name synonymous with all technical things: computing, security, and now even AI. But what happens when we blindly trust the brand more than our own security knowledge? Does the logo always guarantee safety?

The Cofense Phishing Defense Center has identified a new campaign that weaponizes Microsoft's Name and branding to lure users into fraudulent tech support scams. On the surface, this campaign resembles many other scams. However, by using tactics such as social engineering, fake system alerts, and deceptive UI overlays, it becomes a much more in-depth attack.

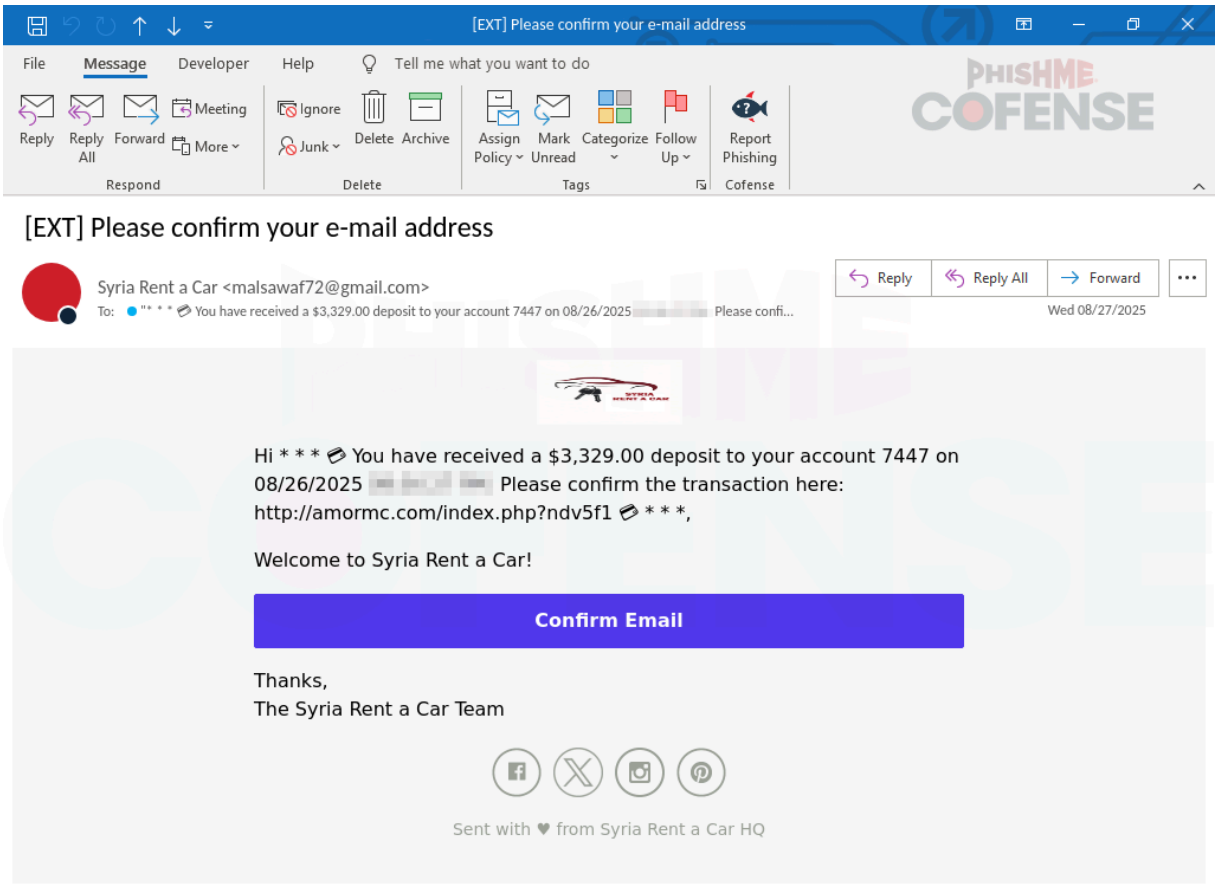


Figure 1: Email Body

The initial email seen in Figure 1 leverages classic scam tactics in an attempt to exploit a recipient's curiosity for financial gain. The threat actor is making the email appear as though it is a reimbursement or payment from *Syria Rent a Car*, promising access to the funds if the recipient "confirms" their email address. Often called a "payment lure", this is a tactic where the threat actor dangles a fake deposit as a pretext to trick the recipient into interacting with the malicious link. While effective payment lures are often not the main goal and are usually a precursor to further compromises, including credential theft or malware delivery.

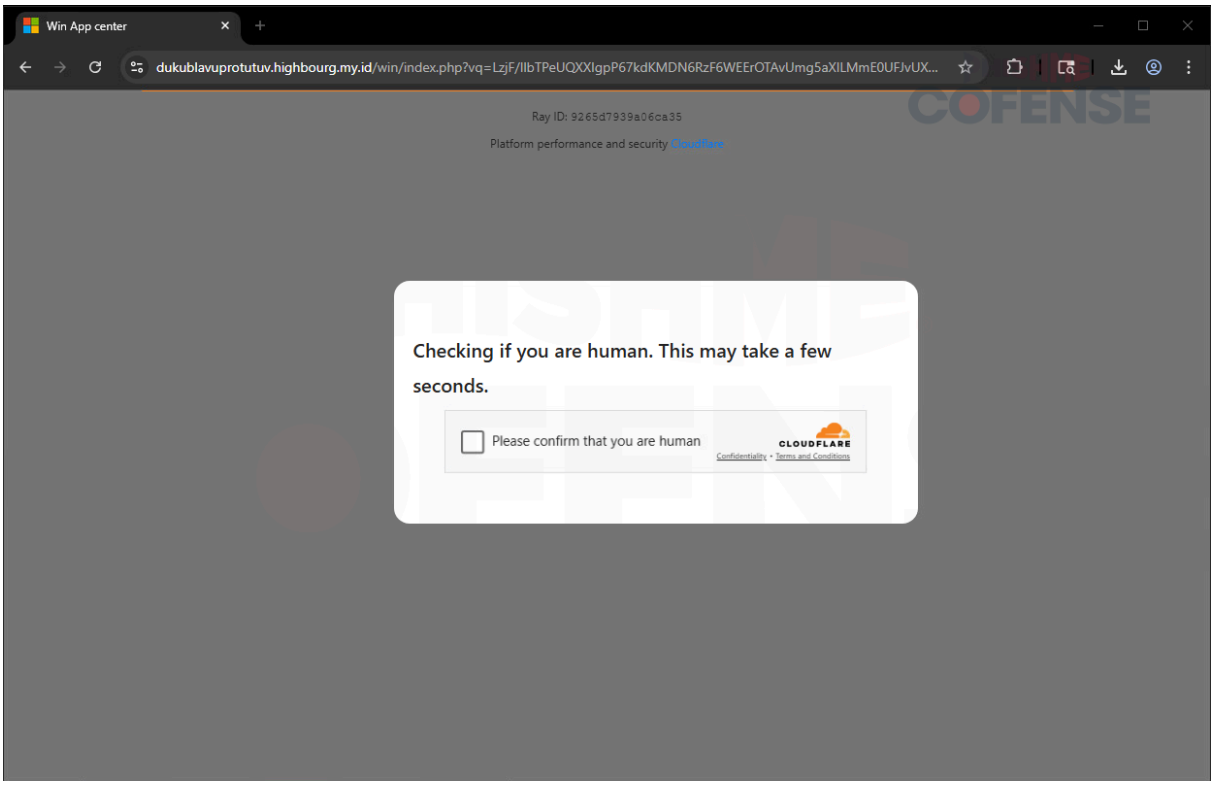


Figure 2: Redirect Page

Upon clicking the link within the email, the user is taken to a fake CAPTCHA challenge where they are asked for human verification. This is another tactic used frequently that serves two purposes for the attacker: first, it adds legitimacy by mimicking the look of a common CAPTCHA verification, and second, it forces engagement from the user to move forward, hindering automated analysis. Once the user has been "confirmed," they are once again redirected, this time to the actual landing page.

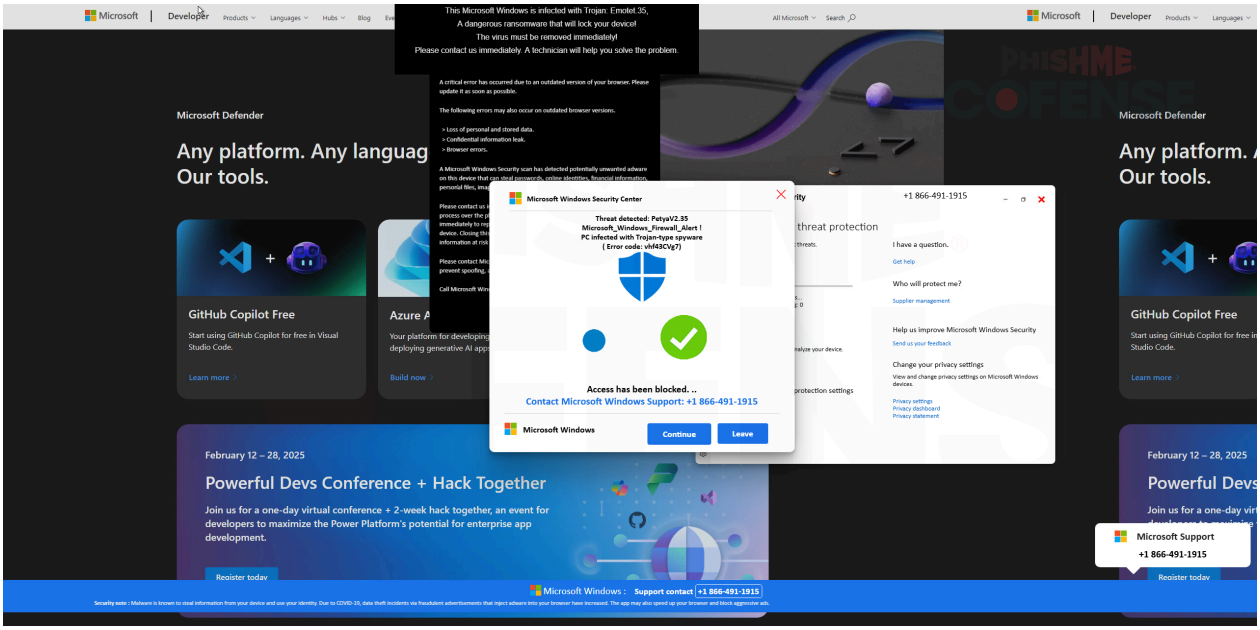


Figure 3: Locked Browser

The final landing page is where this attack goes beyond common scam methods. After passing the captcha verification, the victim is suddenly visually overloaded with several pop-ups that appear to be Microsoft security alerts. Their browser is manipulated to appear locked, and they lose the ability to locate or control their mouse, which adds to the feeling that the system is compromised. This involuntary loss of control creates a faux ransomware experience, leading the user to believe their computer is locked and to take immediate action to remedy the infection. The lock is purely an illusion and can be subverted by holding down the ESC key. By leaning on the familiarity of Microsoft's logos, terminology, and security alert style, while also stripping the victim of control, the threat actor is all but forcing them into calling the "Microsoft Support" number displayed several times on screen. This is likely used as a social engineering ploy to overwhelm and confuse the user, making them think they have been infected and appealing to a sense of urgency that they need to act now. When the victim calls the displayed number, they would be connected to a fake Microsoft support technician, at which point the threat actor could exploit further by asking the user to provide account credentials or persuade the user to install remote desktop tools, allowing full access to their system.

This campaign underscores how brand trust can be weaponized against users by combining familiar scam tactics such as payment lures and fake CAPTCHA's with more advanced methods like fraudulent Microsoft overlays and phone-based social engineering. The threat actor's goal is clear: exploitation by any means necessary to steal information and infiltrate systems.

By employing multiple security layers, awareness training, and encouraging vigilance across organizations, our goal as security professionals at Cofense is also clear: to defend. Our Phishing Detection and Response platform provides organizations with comprehensive phishing defense by allowing them to rapidly detect, investigate, and remediate user-reported phishing threats that evade perimeter defenses. Request a demo today to learn more about how Cofense can help your organization neutralize phishing threats such as this one.

Stage 1 - Observed Infection URL(s):	Infection URL IP(s):
hxxps://alphadogprinting[.]com/index.php?8jl9lz	107[.]180[.]26[.]155 184[.]168[.]97[.]153
hxxp://amormc[.]com/index[.]php?ndv5f1	
hXXp://amormc[.]com/index[.]php?3xmvgr	

Stage 2 - Observed Payload URL(s):	Payload IP(s):
hxxps://my[.]toruftuiov[.]com/9397b37a-50c4-48c0-899d-f5e87a24088d	104[.]21[.]32[.]1
hxxps://shilebatablurap[.]highbourg[.]my[.]id/win/index[.]php?	104[.]21[.]112[.]1
hxxps://nasubutrachat[.]highbourg[.]my[.]id/win/index[.]php?	104[.]21[.]64[.]1
hxxps://blutrecheshetrubler[.]highbourg[.]my[.]id/win/index[.]php	104[.]21[.]16[.]1
hxxps://dukublavuprotutuv[.]highbourg[.]my[.]id/win/index[.]php	104[.]21[.]80[.]1
hXXps://deprivy[.]stified[.]sbs/proc[.]php	104[.]21[.]48[.]1

hXXps://chubagledivepreli[.]highbourg[.]my[.]id/win/index[.]php?	104[.]21[.]96[.]1 18[.]160[.]41[.]101 18[.]160[.]41[.]15 104[.]21[.]32[.]1 104[.]21[.]112[.]1 104[.]21[.]64[.]1 104[.]21[.]16[.]1 104[.]21[.]80[.]1 99[.]198[.]106[.]197