COMODO LABORATUVARLARI WHATSAPP KULLANICILARINI UYARDI:

WhatsApp'a malware saldırısı başladı

Siber güvenlikte dünya lideri Comodo, dünya çapında 900 milyonu aşan WhatsApp kullanıcılarını yeni bir saldırıya karşı uyardı. Siber suçlular, rasgele kişilerin hedeflendiği bir kimlik avı kampanyası kapsamında resmi WhatsApp içeriği gibi görünen sahte e-postalar göndermeye başladı. Mesaja tıklandığında kötü amaçlı yazılım bilgisayarlara ya da telefonlara bulaşarak bütün kişisel bilgileri ve dosyaları ele geçiriyor.

Dünyanın lider siber güvenlik markası Comodo, siber saldırganlara karşı güvenlik çözümleri üretmeye devam ediyor. Comodo Antispam Laboratuvarları (CASL) son olarak, sayıları 900 milyonu aşan WhatsApp kullanıcılarını hedef alan bir saldırıyı tespit etti.
Comodo Antispam Laboratuvarları ekipleri; yeni saldırıyı IP, alan adı ve URL analizlerinden yararlanarak ortaya çıkardı. Yeni yöntemde, siber saldırganlar, rastgele kişilerin hedeflendiği kimlik avı (phishing) kampanyası kapsamında, kötü amaçlı yazılımı (malware) yaymak için resmi WhatsApp içeriği gibi görünen sahte e-postalar gönderiyor. "Mesaj"a tıklandığında kötü amaçlı yazılım bilgisayarlara ya da telefonlara bulaşmış oluyor.

E-postalar, "WhatsApp" olarak bir şemsiye marka adı altında gizlenmiş şekilde sahte bir adresten geliyor, ama "kimden" kısmına dikkatle bakıldığında e-postanın aslında WhatsApp'tan gelmediği kolayca anlaşılıyor.

"Comodo hep siber suçlulardan bir adım önde"
Comodo ve Comodo Antispam Laboratuvarları Teknoloji Direktörü Fatih Orhan, saldırganların giderek pazarlamacılara daha da çok benzemeye başladığını belirterek, "Durumdan habersiz kullanıcıların e-postaları açıp kötü amaçlı yazılımı yaymasını sağlamak için yaratıcı konu satırları kullanmaya çalışıyorlar. Comodo, siber suçluların hep bir adım önünde olan yenilikçi teknolojiler yaratmak, uç noktaları koruyup güvenlik altına almak ve hem işletmeleri hem de BT ortamlarını güvenli tutmak için canla başla çalışıyor. Bunu da büyük bir başarıyla gerçekleştiriyor" diye konuştu.

Konu satırları rastgele karakter dizisiyle bitiyor
Comodo Antispam Laboratuvarları, siber saldırganların, bu kötü amaçlı yazılımı yaymak ve bilgisayarlara bulaştırmak için yazdıkları e-postalardaki konu satırlarının her birinin, 'xgod' ya da 'Ydkpda' gidi rastgele bir karakter dizisiyle bittiğini tespit etti. Bunların bazı verileri kodlayarak alıcıları belirlemek için kullanıldığı değerlendiriliyor.

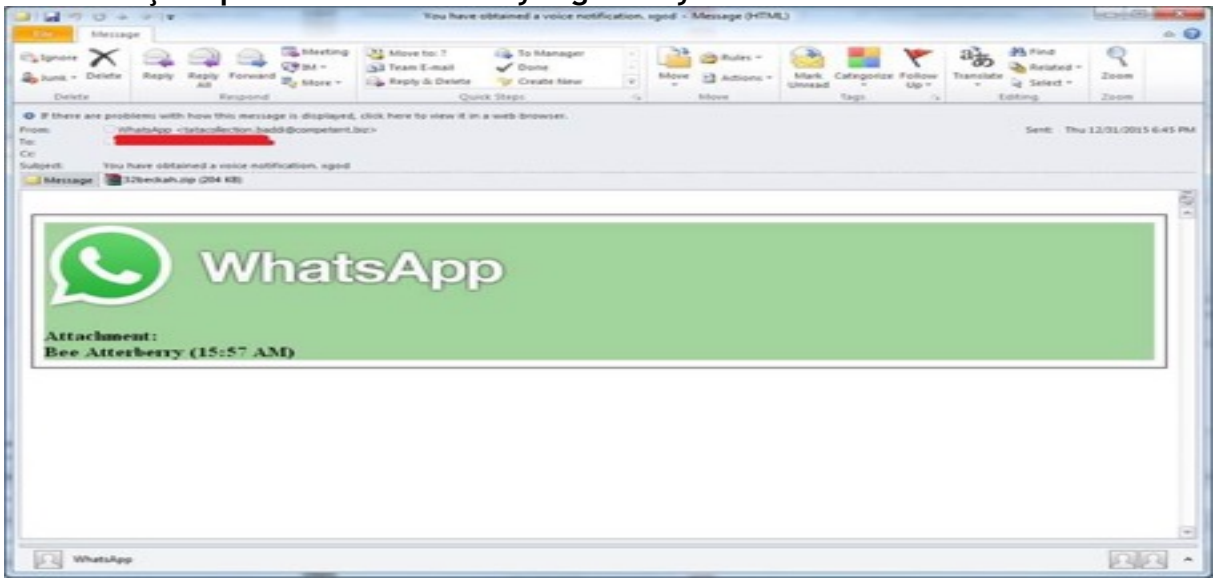
Otomatik açılan bir uygulamaya ekleniyor
Konu satırlarının ek kısmında, kötü amaçlı yazılımın yürütülebilir (.exe) dosyasının yer aldığı bir sıkıştırılmış (zip) dosya bulunuyor. Söz konusu kötü amaçlı yazılım,

"Nivdort" ailesinin bir varyantı. Bu kötü amaçlı yazılım çoğu zaman kendini farklı sistem klasörleri içine kopyalıyor ve bilgisayarın kayıt defterinde otomatik açılan bir uygulamaya kendini ekliyor. E-posta ekindeki zip dosyası açılıp çalıştırıldığında, kötü amaçlı yazılım bilgisayara geçmiş oluyor.

İşte o konu satırları:
Bir sesli bildirim aldınız xgod
Bir sesli mesaj kaçırdınız. Ydkpda
Kısa bir ses kaydı alındı! Jsvk
Kısa bir sesli kayıt alındı npulf
Bir sesli bildirim alındı sqdw
Bir video bildiriminiz var. Eom
Kısa bir video mesajı alındı. Atjvqw
Kısa süre önce bir sesli mesaj aldınız. Yop

COMODO ANTİSPAM LABORATUVARLARI
Comodo Antispam Laboratuvarları ekibi 40'tan fazla BT güvenlik uzmanı, etik korsan (hacker) ve bilgisayar bilimcisi ve mühendisinden oluşuyor. Her biri tam zamanlı Comodo çalışanı olan ekip üyeleri dünyanın dört bir yanından gelen istenmeyen e-postaları (spam), kimlik avı (phishing) amaçlı uygulamaları ve kötü amaçlı yazılımları (malware) analiz edip filtreliyor. ABD, Türkiye, Ukrayna, Filipinler ve Hindistan'da ofisleri bulunan CASL ekibi günde 1.000.000'dan fazla potansiyel kimlik avı, spam ve diğer kötü amaçlı/istenmeyen e-postayı analiz ediyor. Bunu yaparken kendi müşteri tabanını ve genel olarak halkı, işletmeleri ve internet topluluğunu korumak ve güvenli tutmak için elindeki tüm bulgu ve öngörülerden faydalanıyor. BT ortamının kimlik avı amaçlı uygulamaların, kötü amaçlı yazılımların, casus yazılımların saldırısı altında olduğunu veya diğer siber saldırı türlerine maruz kaldığını düşünen şirketler, https://enterprise.comodo.com/contact-us.php adresinden Comodo güvenlik danışmanlarına ulaşabilir.

Kötü amaçlı e-postalar ekranda böyle görünüyor:



Daha fazla bilgi almak için, medya mensupları ve analistler aşağıdaki ilgililerle temasa geçebilir:

Banu Buyurgan
GTC İletişim Danışmanlığı
+90 312 447 00 20
banu.buyurgan@gtc.com.tr