OUCH!

تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

# میلویئر کو روکیں

## جائزہ

جب سائبر سکیورٹی کی بات ہوتی ہے تو آپ نے شاید وائرس، ٹروجن، رینسم ویئر یا روُٹ کٹ جیسی اصطلاحات سُنی ہوں گی- یہ مُضر پروگرامز کی مختلف اقسام ہیں جو کہ میلویئر کہلاتی ہیں اور سائبر مُجرمان اس کے ذریعے کمپیوٹرز اور دوسرے آلات کو متاثر کرتے ہیں- ایک بار میلویئر جب انسٹال ہو جائے تو وہ اس کے ذریعے کچھ بھی کر سکتے ہیں- آپ میلویئر، اس سے بچاؤ کی تدابیر اور سب سے اہم ان اقدامات کے بارے میں جانیں جن کے ذریعے آپ ان سے اپنی حفاظت کر سکتے ہیں-

## میلویئر کیا ہے؟

آسان الفاظ میں میلویئر ایک سافٹ ویئر، ایک کمپیوٹر پروگرام ہوتا ہے جس کے ذریعے آپ غیر مجاز کام سر انجام دے سکتے ہیں- یہ دو الفاظ کا مجموعہ ہے یعنی کہ میلویئر اور سافٹ ویئر- سائبر مُجرمان آپ کے کمپیوٹرز یا آلات میں میلویئر اس لیئے انسٹال کرتے ہیں تاکہ وہ ان کا اختیار حاصل کر سکیں- ایک بار انسٹال ہونے کے بعد میلویئر مُجرمان کو آپ کی آن لائن سرگرمیوں پر نظر رکھنے کی صلاحیت فراہم کر دیتے ہیں، آپ کے پاس ورڈز یا فائلز چرا سکتے ہیں یا آپ کے سسٹم کو استعمال کرتے ہوئے دوسروں پر حملہ کر سکتے ہیں- میلویئر آپ کی فائلز کا بھی اختیار سنبھال سکتا ہے اور پھر آپ سے اس اختیار کو واپس لینے کے لیئے تاوان کا مطالبہ کرتا ہے- کئی لوگوں کو لگتا ہے کہ میلویئر کا مسئلہ صرف ونڈوز کمپیوٹرز کے ساتھ ہے لیکن بدقسمتی سے میلویئر میک کمپیوٹرز اور اسمارٹ فونز سے لے کر ڈی وی آر اور سکیورٹی کیمرے تک ہر آلہ کو متاثر کر سکتا ہے- سائبر مُجرمان جتنے زیادہ کمپیوٹرز اور آلات کو متاثر کریں گے، اتنے ہی زیادہ پیسے کمائیں گے- لہٰذا ان کے لیئے آپ سمیت ہر کوئی ہدف ہے-

## اپنی حفاظت کریں - میلویئر کو روکیں

آپ کو شاید ایسا لگتا ہو کہ میلویئر سے متاثر ہونے سے بچنے کے لیئے آپ کو صرف اینٹی وائرس سافٹ ویئر جیسے سکیورٹی پروگرام کو انسٹال کرنا ہوگا لیکن بد قسمتی سے اینٹی وائرس ہر میلویئر کو نہیں روک سکتا ہے- سائبر مُجرمان مستقل ایسے نئے اور نفیس میلویئر تخلیق کر رہے ہیں جن کا پکڑا جانا بہت مشکل ہے- دوسری جانب، اینٹی وائرس وینڈرز مستقل اپنی مصنوعات کو میلویئر کی شناخت کرنے کی نئی صلاحیات سے اپڈیٹ کرتے رہتے ہیں- یہ ایک طرح سے ہتھیار کی دوڑ بن گئی ہے اور بُرے لوگ اس میں ایک قدم آگے ہی ہوتے ہیں- آپ اپنی حفاظت کے لیئے چونکہ صرف اینٹی وائرس پر بھروسہ نہیں کر سکتے ہیں اس لیئے مندرجہ ذیل اضافی اقدامات اٹھائیں:

سائبر مُجرمان اکثر آپ کے کمپیوٹرز اور آلات کے سافٹ ویئر میں موجود کمزوریوں کا فائدہ اٹھا کر اُنہیں متاثر کر دیتے ہیں- آپ کا سافٹ ویئر جتنا تازہ ترین ہو گا، آپ کے سسٹم میں اُتنی ہی کم کمزوریاں ہوں گی اور سائبر مُجرمان کے لیئے اُنہیں متاثر کرنا اُتنا ہی مشکل ہو گا- آپ اس بات کو یقینی بنائیں کہ آپ کے آپریٹنگ سسٹمز، ایپلیکیشنز، براؤزر اور براؤزر پلگ اِنز اور آلات ہمیشہ اپڈیٹ رہیں اور اُن میں تازہ ترین ورژن چل رہا ہو- اس بات کو یقینی بنانے کے لیئے جب بھی مُمکن ہو، آپ خودکار اپڈیٹ کو فعّال کر دیں-

ایک عام طریقہ جس کے ذریعے سائبر مُجرمان کمپیوٹرز یا موبائل آلات کو متاثر کرتے ہیں وہ یہ ہے کہ وہ جعلی کمپیوٹر پروگرامز یا موبائل ایپلیکیشنز بنا کر اُنہیں انٹرنیٹ پر شائع کرتے ہیں اور پھر دھوکہ دہی کے ذریعے آپ سے اُنہیں ڈاؤن لوڈ اور پھر انسٹال کرواتے ہیں- آپ پروگرامز یا ایپلیکیشنز کو صرف قابل بھروسہ آن لائن اسٹورز سے ڈاؤن لوڈ کریں- آپ اپنے آپ کو اُن موبائل ایپلیکیشنز سے بھی دُور رکھیں جو بالکل نئی ہوں یا جن کے بارے میں بہت کم مثبت تبصرے موجود ہوں یا جو بہت کم اپڈیٹ ہوتی ہوں یا جنہیں بہت کم تعداد میں لوگوں نے ڈاؤن لوڈ کیا ہو- اگر آپ کسی کمپیوٹر پروگرام یا موبائل ایپلیکیشن کو مزید استعمال نہیں کر رہے ہیں تو اُسے حذف کر دیں-

سائبر مُجرمان اکثر لوگوں سے دھوکہ دہی کے ذریعے میلویئر انسٹال کروا دیتے ہیں- مثال کے طور پر وہ آپ کو ایسی ای میل بھیج سکتے ہیں جو کہ دیکھنے میں صحیح لگ رہی ہوتی ہے اور اُس میں ایک اٹیچمنٹ یا لنک موجود ہوتا ہے- اکثر ایسا لگتا ہے کہ یہ ای میل آپ کے بینک یا دوست کی جانب سے آئی ہے تاہم اگر آپ اس فائل کو کھولتے ہیں یا لنک پر کلک کرتے ہیں تو آپ ایک مُضر کوڈ کو مُتحرّک کر دیتے ہیں جس کے ذریعے میلویئر آپ کے سسٹم میں انسٹال ہو جاتا ہے- اگر کوئی ای میل شدید عُجلت کا احساس دلاتی ہے یا صحیح نہیں لگ رہی ہوتی ہے تو ہو سکتا ہے کہ یہ ایک حملہ ہو- آپ ہمیشہ محتاط رہیں کیوں عام فہم اکثر آپ کا سب سے بہترین دفاع ہوتا ہے-

آپ اپنے سسٹم اور فائلز کا باقاعدگی سے کلاؤڈ پر موجود سروسز پر بیک اپ لیتے رہیں یا اُن بیک اپس کو آف لائن ذخیرہ کریں جیسے کہ منقطع کی ہوئی ایکسٹرنل ڈرائیوز پر- یہ آپ کے بیک اپس کی اُس صورت میں حفاظت کرتا ہے جب کوئی میلویئر اُسے انکرپٹ یا حذف کرنے کی کوشش کرتا ہے- بیک اپس بہت اہم ہوتے ہیں، یہ اکثر میلویئر سے متاثر ہونے کے بعد بحالی کا واحد ذریعہ رہ جاتے ہیں-

بالآخر میلویئر سے دفاع کا سب سے بہترین طریقہ اپنے تمام سافٹ ویئر اور آلات کو اپڈیٹ رکھنا، اُن میں قابل بھروسہ اینٹی وائرس سافٹ ویئر انسٹال کرنا اور کسی بھی شخص کے دھوکہ دہی کے ذریعے آپ کے سسٹم کو متاثر کرنے کی کوشش کرنے سے ہوشیار رہنا شامل ہے- اگر پھر بھی آپ کسی حملے کا شکار ہوتے ہیں تو اس صورت میں بیک اپس اپنی معلومات کو بحال کرنے کا واحد ذریعہ رہ جاتا ہے-

## اردو ایڈیشن

Rewterz پاکستان کی معروف انفارمیشن سکیورٹی کمپنی ہے جو پچھلے سات سالوں سے آئی ٹی سکیورٹی کے شعبے میں خدمات سرانجام دے رہی ہے - کمپنی کے بارے میں مزید معلومات کے لئے http://www.rewterz.com کا دورہ کریں یاہمارے فیس بک پیج https://www.facebook.com/Rewterz کو 'لائک' کریں یا ٹوئیٹر @Rewterz پر فالو کریں-

## مہمان مُدیر

لینی زیلٹسر مینروہ لیبس میں میلویئر سے نمٹنے سے متعلق اینڈ پوائنٹ مصنوعات بناتے ہیں اور SANS انسٹیٹیوٹ میں پڑھاتے ہیں- لینی، ٹوئیٹر پر @lennyzeltser کے ذریعے فعّال ہوتے ہیں اور وہ zeltser.com پر سکیورٹی کا بلاگ لکھتے ہیں-

## وسائل:

رینسم ویئر: https://www.sans.org/u/EdI

بیک اپس: https://www.sans.org/u/EdN

فِشنگ کو روکیں: https://www.sans.org/u/EdS