مارچ ۲۰۱۶ OUCH!

کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- میلویئر کیا ہے؟
- میلویئرکیا ہے ؟
- میلویئر کون بناتا ہے؟

میلویئر کیا ہے

جائزہ

جب سائبر سکیورٹی کی بات ہوتی ہے تو آپ نے یہ اصطلاحات سُنی ہوں گی جیسے کہ وائرس، ٹروجن ، رینسم ویئر یا رُوٹ کٹ۔ یہ تمام الفاظ ایک ہی چیز بیان کرتے ہیں یعنی وہ پروگرامز جو کہ سائبر مُجرمان کمپیوٹرز یا آلات کو متاثر کرنے کے لیئے استعمال کرتے ہیں۔ ایک عام اصطلاح جو کہ ان مختلف پروگرامز کو بیان کرنے کے لیئے استعمال ہوتی ہے وہ لفظ «میلویئر» ہے۔ نیوزلیٹر کے اس شمارے میں ہم یہ بتائیں گے کہ میلویئر کیا ہے، اسے کون تخلیق کرتا ہے اور کیوں، اور سب سے اہم بات یہ کہ آپ کن اقدامات کے ذریعے ان سے اپنی حفاظت کر سکتے ہیں۔

مہمان ایڈیٹر

لینی ذیلٹسر، NCR Corp میں اپنی توجہ صارفین کے آئی ٹی آپریشنز کی حفاظت پر مرکوز رکھتے ہیں اور SANSانسٹیٹیوٹ میں میلویئر کی روک تھام کے بارے میں تربیت دیتے ہیں۔ لینی ٹوئیٹر پر @lennyzeltser کے ذریعے فعال ہیں اور وہ سکیورٹی کے بلاگ blog.zeltser.com پہ لکھتے ہیں۔

میلویئر کیا ہے؟

میلویئر صرف ایک سافٹ ویئر ہے، ایک کمپیوٹر پروگرام، جو کہ غلط سرگرمیوں کے لیئے استعمال ہوتا ہے۔ درحقیقت میلویئر کی اصطلاح دو الفاظ یعنی کہ «میلیشیئس» اور «سافٹ ویئر» کا مجموعہ ہے۔ سائبر مُجرمان آپ کے کمپیوٹر یا آلات میں میلویئر انسٹال کرتے ہیں تاکہ اُن پر اختیار حاصل کر سکیں یا اُن میں موجود معلومات تک رسائی حاصل کر سکیں۔ ایک بار میلویئر انسٹال ہو جائے تو یہ لوگ آپ کی آن لائن سرگرمیوں کی جاسوسی کر سکتے ہیں، آپ کی فائلز یا پاسورڈ چرُا سکتے ہیں۔ میلویئر آپ کو اپنی ہی فائلز تک رسائی سے محروم کر سکتے ہیں اور اُن تک واپس رسائی کے لیئے آپ سے حملہ آور کے لیئے تاوان طلب کرتے ہیں۔

کئی لوگوں کو یہ غلط فہمی ہے کہ میلویئر صرف ونڈوز کمپیوٹرز کے لیئے مسئلہ ہے، ونڈوز چونکہ سب سے زیادہ استعمال ہوتی ہے اس لیئے وہ سب سے زیادہ نشانہ بنتی ہے لیکن کسی بھی آلہ کو متاثر کر سکتی ہے جس میں میک، فونز، اسمارٹ فونز یا ٹیبلٹس بھی شامل ہیں۔ سائبر مُجرمان جتنے زیادہ آلات کو متاثر کرتے ہیں اتنے پی زیادہ پیسے کما سکتے ہیں۔ اس لیئے میلویئر کا نشانہ ہر کوئی بن سکتا ہے بشمول آپ کے۔

میلویئر کون بناتا ہے؟

میلویئر کو اب شوقیہ ہیکر یا مُتجسس لوگ ہی نہیں بلکہ بہت ہی نفیس سائبر مُجرمان بھی بناتے ہیں، اُن کا مقصد آپ کے کمپیوٹر یا آلہ کے ذریعے پیسے بنانا ہے شاید آپ سے چرائی ہوئی معلومات بیچ کر، اسپیم ای-میلز بھیج کر، ڈینائل آف سروس کے حملوں کے ذریعے یا بھتاخوری کے ذریعے۔ جو لوگ میلویئر کو بناتے ہیں، اُسے دوسروں میں تقسیم کرتے ہیں اور اُس سے فائدہ اٹھاتے ہیں، وہ ایک انفرادی شخص سے لے کر مُجرمان کے منظم گروہ، یہاں تک کہ سرکاری تنظیم میں سے کوئی بھی ہو سکتا ہے۔ جو لوگ آج کے دور میں بہت نفیس میلویئر تخلیق کر

میلویئر کیا ہے

رہے ہیں وہ اکثر ایسے ہوتے ہیں جو خُصوصا اس کام کے لیئے مُختص ہوتے ہیں اور وہ کُل وقتی ملازمت کے طو ر پر میلویئر بناتے ہیں۔ مزید یہ کہ جب وہ ایک میلویئر بنا لیتے ہیں تو اکثر اُسے دُوسرے لوگوں یا تنظیموں کو بیچنے کی کوشش کرتے ہیں اور اپنے «صارفین» کو باقاعدگی سے اپڈیٹس اور سپورٹ بھی فراہم کرتے ہیں۔

آپ میلویئر سے اپنی حفاظت کے لیئے مشکوک پیغامات کے بارے میں مُتشکّک رہیں، اپنے آلات کو اپڈیٹ رکھیں اور جب بھی مُمکن ہو تازہ ترین اینٹی وائرس انسٹال کریں۔

اپنی حفاظت کرنا

اپنی حفاظت کرنے کے لیئے سب سے عام قدم، قابل بھروسہ ونڈر کا اینٹی وائرس سافٹ ویئر انسٹال کرنا ہے۔ ایسے ٹوُلز جو اینٹی میلویئر سافٹ ویئر بھی کہلاتے ہیں۔ اس طرح تخلیق کیئے جاتے ہیں تاکہ وہ میلویئر کو پکڑ سکیں اور اُسے روک سکیں۔ تاہم اینٹی وائرس تمام مُضر پروگرامز کو روک نہیں سکتے ہیں، سائبر مُجرمان مُستقل جدت لاتے جا رہے ہیں اور ایسے نفیس میلویئر تخلیق کر رہے ہیں جن کو پکڑا نہیں جا سکتا ہے۔ نتیجتا اینٹی وائرس ونڈرز مُستقل اپنی مصنوعات کو اپڈیٹ کے ذریعے نئی صلاحیتوں سے لیس کرتے رہتے ہیں تاکہ میلویئر کو پکڑا جا سکے۔ یہ ایک طرح کی دوڑ بن گئی ہے جس میں دونوں فریق ایک دوُسرے کو نیچا دکھانے کی کوشش کرتے ہیں۔ بد قسمتی سے بُرے لوگ ایک قدم آگے ہی ہوتے ہیں۔ آپ چونکہ صرف اینٹی وائرس پر بھروسہ نہیں کر سکتے ہیں اس لیئے آپ کو اُن مُندرجہ ذیل اقدامات کو اپنا کر اپنے آپ کو محفو ظ بنانا چاہیئے۔

- سائبر مُجرمان اکثر کمپیوٹر یا آلات کے سافٹ ویئر میں موجود کمزوری کا فائدہ اُٹھاتے ہوئے اُنھیں متاثر کر دیتے ہیں۔ آپ کا سافٹ ویئر جتنا ہلکا ہوگا اس کے سسٹم میں اُتنی ہی کم کمزوریاں ہوں گی اور سائبر مُجرمان کے لیئے اسے متاثر کرنا مُشکل ہوگا۔ اس لیئے آپ اس بات کو یقینی بنائیں کہ آپ کے آپریٹنگ سسٹم، ایپلیکیشنز اور آلات میں خوُدکار اپڈیٹس کی انسٹالیشن فعال ہوں۔
- ایک عام طریقہ جس کے ذریعے سائبر مُجرمان موبائل آلات کو متاثر کرتے ہیں وہ جعلی موبائل ایپلیکیشنز بنانا، اُسے انٹرنیٹ پر شائع کرنا اور پھر لوگوں کو دھوکہ دہی کے ذریعے اُسے ڈاؤن لوڈ اور انسٹال کروانا ہے۔ آپ ایپلیکیشنز کو صرف قابل اعتماد آن لائن اسٹورز سے ڈاؤن لوڈ اور انسٹال کریں۔ اس کے علاوہ یہ کہ آپ صرف اُس موبائل ایپلیکیشن کو انسٹال کریں جو کہ کافی عرصہ سے آن لائن شائع ہوچُکی ہے، اُنھیں کافی لوگ ڈاؤن لوڈ کر چُکے ہیں اور اس کے کافی سارے مثبت جائزے موجود ہیں۔
- کمپیوٹرز پر ایک اسٹینڈرڈ اکاؤنٹ استعمال کریں جس کے پاس محدود اختیارات ہوں بجائے اُن اکاؤنٹس کے جن کے پاس زیادہ اختیارات ہوں جیسے کہ «ایڈمنسٹریٹر» اور «رُوٹ» اکاؤنٹس۔ یہ مختلف اقسام کے میلویئر کو خودبخود انسٹال ہونے سے روک کر اضافی تحفظ فراہم کرتا ہے۔
- سائبر مُجرمان اکثر لوگوں کو دھوکہ دہی کے ذریعے میلویئر انسٹال کرواتے ہیں۔ مثال کے طور پر وہ آپ کو ایسی ای-میل بھیج سکتے ہیں جو کہ بالکل صحیح لگ رہی ہو اور اُس میں ایک اٹیچمنٹ یا لنک ہو۔ وہ ای-میل ایسی لگتی ہے جیسے آپ کے بینک یا دوست کی جانب سے آئی ہو۔ تاہم اگر آپ کوئی فائل ڈاؤن لوڈ کرتے ہیں یا کسی لنک کو کلک کرتے ہیں تو آپ اُس مضر کوڈ کو فعال کر دیتے ہیں جو کہ آپ کے سسٹم میں میلویئرانسٹال کر دیتا ہے۔ اگر کوئی پیغام بہت زیادہ عُجلت کا احساس دلا رہا ہو، مُبہم ہو یا

میلویئر کیا ہے

حقیقت کے منافی لگ رہا ہو تو مُمکن ہے کہ یہ حملہ ہو۔ آپ مشکوک رہیں کیونکہ اکثر اپنی عقل سلیم کا استعمال آپ کا بہترین دفاع ہوتا ہے۔

- آپ اپنے سسٹم اور فائلز کا کلاؤڈ پر مبنی سروسز پر باقاعدگی سے بیک اپ لیتے رہیں یا اپنے بیک اپ کو آف لائن، جیسے کہ مُنقطع شُدہ بیرونی ڈرائیو، پر ذخیرہ کرتے رہیں۔ یہ آپ کے بیک اپس کو اُس صورت میں محفوظ رکھتا ہے جب کوئی میلویئر اُسے انکرپٹ یا مٹانے کی کوشش کرتا ہے۔ بیک اپ بہت اہم ہوتے ہیں، یہ اکثر وہ واحد راستہ ہو تا ہے جس کے ذریعے آپ میلویئر انفیکشن سے روُبصحت ہو سکتے ہیں۔

بالآخر میلویئر سے دفاع کا سب سے بہترین طریقہ یہ ہے کہ آپ اپنے سافٹ ویئر کا جدید ترین ورژن استعمال کریں، مشہوُر وینڈر کے ذریعے قابل بھروسہ اینٹی وائرس سافٹ ویئر انسٹال کریں اور کسی بھی شخص کے آپ کو بیوقوف بنانے یا آپ کو دھوکہ دہی کے ذریعے آپ کے اپنے سسٹم کو متاثر کرنے سے ہوشیار رہیں۔

مزید جانیئے

OUCH! کے ماہانہ سیکیورٹی تعلیم کے نیوز لیٹر کو سبسکرائب کریں،OUCH! archives تک رسائی حاصل کریں اورSANS سیکیورٹی سے مزیدآگاہی کے لئے اس ویب سائٹ کا دورہ کریں http://www.securingthehuman.org (انگریزی میں) ۔

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۔

وسائل:

فشنگ: https://securingthehuman.sans.org/ouch/2015#december2015

سوشل انجینئرنگ: https://securingthehuman.sans.org/ouch/2014#november2014

موبائل ایپلیکیشنز کا محفوظ استعمال: https://securingthehuman.sans.org/ouch/2015#january2015

اپنے نئے ٹیبلیٹ کو محفوظ بنانا: https://securingthehuman.sans.org/ouch/2016#january2016

بیک اپس: https://securingthehuman.sans.org/ouch/2015#august2015

ایڈیٹوریل بورڈ: بل وے مین، والٹ اسکریونز، فل ہوفمن، لینس اسپڑنر، کارمن رولی ہارڈی۔

ترجمہ: شعیب ہاشمی