کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سیکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- میل ویئر کیا ہے
- کون اور کیوں؟
- اپنے آپ کو محفوظ رکھنا

میل ویئر کیا ہے

جائزہ

جب لوگ سائبر سیکیورٹی کے بارے میں بات کرتے ہیں تو آپ نے شاید یہ اصطلاحات سنی ہوں جیسے کہ وائرس، ورم، ٹروجن یا رُوٹ کٹ- یہ اصطلاحات مختلف اقسام کے پروگرامز، جوکہ سائبر مجرمان کمپیوٹر یا موبائل آلات کو متاثر کرنے یا اُن پر قبضہ کرنے کیلئے استعمال کرتے ہیں، کوبیان کرنے کیلئے استعمال ہوتی ہیں - آج یہ مختلف اصطلاحات میل ویئر کہلاتی ہیں۔ اس نیوز لیٹر میں ہم آپ کو بتائیں گے کہ میل ویئر کیا ہے، اسے کون اور کیوں بناتا ہے اور آپ اپنے آپ کو اُس سے کیسے محفوظ رکھ سکتے ہیں۔

مہمان ایڈیٹر

لینی ذیلٹسر OUCH کے اس شمارے کے مہمان ایڈیٹر ہیں۔ لینی ، NCR Corp میں اپنی توجہ صارفین کے آئی ٹی آپریشنز کی حفاظت پر مرکوز رکھتے ہیں اور SANS انسٹیٹیوٹ میں میل ویئر کی روک تھام کے بارے میں تربیت دیتے ہیں۔ لینی ٹوئیٹر پر @lennyzeltser کے ذریعے فعال ہیں اور وہ سیکیورٹی کے بلاگ blog.zeltser.com پہ لکھتے ہیں۔

میل ویئر کیا ہے؟

سادہ الفاظ میں یہ کہ میل ویئر ایک سافٹ ویئر، ایک کمپیوٹر پروگرام ہوتا ہے جسکے ذریعے بدنیتی پر مبنی کاروائیاں سر انجام دی جاتی ہیں۔ درحقیقت میل ویئر کی اصطلاح «میلیشیئز» اور «سافٹ ویئر» کے الفاظ کا مجموعہ ہے۔ سائبر مجرمان کا اصل مقصد آپ کے کمپیوٹرز یا موبائل آلات پر میل ویئر انسٹال کرنا ہے۔ ایک بار میل ویئر انسٹال ہوجائے تو پھر یہ ہیکرز ممکنہ طور پر اُس کا مکمل اختیار حاصل کر سکتے ہیں۔ کئی لوگوں کو یہ غلط فہمی ہے کہ میل ویئر کا مسئلہ صرف ونڈوز کمپیوٹرز کے ساتھ ہے۔ ونڈوز کا چونکہ استعمال زیادہ ہے، اسی لئے وہ بڑا ہدف بھی ہے۔ میل ویئر اسمارٹ فون اور ٹیبلٹ سمیت کسی بھی کمپیوٹنگ آلے کو متاثر کر سکتا ہے۔ درحقیقت موبائل آلات پر مُضر سافٹ ویئر کا اثر مسلسل بڑھ رہا ہے۔ اسکے علاوہ اس بات کو بھی یاد رکھیں کہ آپ سمیت کوئی بھی اُس کا ہدف بن سکتاہے۔ جتنے زیادہ کمپیوٹرز اور موبائل آلات کو سائبر مجرمان متاثر کریں گے اُتنا زیادہ وہ اُس سے پیسہ کمائیں گے۔ مجرمان اس بات کی پرواہ نہیں کرتے ہیں کہ وہ کسے متاثر کر رہے ہیں، بس وہ زیادہ سے زیادہ لوگوں کو متاثر کرنے کی کوشش کرتے ہیں۔

کون اور کیوں؟

میل ویئر کو اب صرف تجسس رکھنے والے یا شوقین ہیکرز ہی تخلیق نہیں کرتے ہیں بلکہ اب اسے بہترین سائبر مجرمان اپنے مخصوص اہداف کو حاصل کرنے کے لئے تخلیق کرتے ہیں۔ ان اہداف میں آپ کی خوفیہ معلومات کو چوری کرنا ، لاگ ان اور پاس ورڈ حاصل کرنا، اسپیم ای میل بھیجنا، ڈینائل آف سروس کا آغاز کرنا، بھتہ خوری یا شناخت چوری کرنا شامل ہو سکتا ہے- مثلاً ایک میل ویئر جو کہ کرپٹ لاکر کے نام سے جانا جاتا ہے، اُسے سائبر مجرمان آپ کے کمپیوٹر کی تمام فائلز کو متاثر اور انکرپٹ کرنے کے لئے استعمال کرتے ہیں۔ ایک بار جب وہ فائلز متاثر اور انکرپٹ ہوجائیں تو یہ سائبر مجرمان تاوان طلب کرتے ہیں اُن فائلز کو ڈیکرپٹ کرنے کے بدلے- جو لوگ یہ میل ویئر تخلیق کرتے ہیں، اُسے تعینات کرتے ہیں اور اُس سے فائدہ اُٹھاتے ہیں، وہ ایک فرد جو کہ یہ سب کچھ انفرادی طور پر کررہا ہو، سے لکر پُر منظم جرائم پیشہ گروہ یا سرکاری تنظیمیں

میل ویئر کیا ہے

ہو سکتی ہیں۔ اسکےعلاوہ آج کل کے بہترین میل ویئر وہ لوگ تخلیق کر رہے ہیں جو کہ خاص طور پر اس مقصد کے لئے وقف ہوتے ہیں یعنی کہ میل ویئر بنانا اُن کا کل وقتی کام ہے۔ درحقیقت جب وہ ایک بار میل ویئر بنالیتے ہیں تو پھر وہ اُسے دوسرے افراد یا تنظیموں کو بیچ دیتے ہیں اور باقاعدگی سے اپنے گاہک کو اپڈیٹ اور سپورٹ فراہم کرتے ہیں۔ ایک بار میل ویئر خریدنے کے بعد مجرمان پیسے کماتے ہیں اُس کو لاکھوں غیر مشتبہ متاثرین کے سسٹم میں انسٹال کرکے، جس کے ذریعے متاثرین کا سسٹم باٹ نیٹ بن جاتا ہے۔ یہ باٹ نیٹ دور سے کنٹرول ہونے والی آرمی بن جاتا ہے جسے سائبر مجرم اپنے مقاصد کے لیے استعمال کرتا ہے یا اُس متاثرہ کمپیوٹر کو دوسرے سائبر مجرمان کو بیچ دیتا ہے۔

اپنے آپ کو میل ویئر سے محفوظ رکھنے کا سب سے بہترین طریقہ اس بات کی یقین دہانی کرنا ہے کہ آپ کے آلات اپڈیٹ ہیں، ہوسکے تو اُن میں موجودہ اینٹی وائرس ہو اور بالآخر آپ حملے کےلئے ہوشیار رہیں۔

اپنے آپ کو محفوظ رکھنا

ایک عام طریقہ اپنے کمپیوٹر اور موبائل آلات کو میل ویئر سے محفوظ رکھنے کا یہ ہے کہ آپ قابلِ اعتماد ونڈر کا اینٹی وائرس سافٹ ویئر انسٹال کریں۔ اینٹی وائرس جو کہ کبھی کبھی اینٹی میل ویئر بھی کہلاتا ہے، ایک سیکیورٹی سافٹ ویئر ہے جو کہ مضر سافٹ ویئر کی شناخت کرنے اور اُسے روکنے کے لیے بنایا گیا ہے۔ تاہم اینٹی وائرس ہر میل ویئر کو روک یا اُس کا خاتمہ نہیں کرسکتا ہے۔ سائبر حملہ آور حملہ کرنے کے لیے مسلسل ایسے نئے اور بہترین طریقے اپنا رہے ہیں اور اُن میں جدت لا رہے ہیں جن کے ذریعے اینٹی وائرس پروگرام سے بچا جا سکتا ہے۔ اس وجہ سے اینٹی وائرس ونڈرز اپنے پراڈیکٹ کو مسلسل ایسی نئی صلاحیتوں سے لیس کررہے ہیں جن کے ذریعے نئے میل ویئر کی شناخت کی جاسکے- کئی طرح سے یہ ہتھیار کی دوڑ بن گئی ہے جس میں دونوں فریقین ایک دوسرے کو مات دینے کی کوشش کرتی ہیں- بد قسمتی سے سائبر مجرمان کو ہمیشہ سے ہی برتری حاصل رہی ہے- آپ اس بات کو یاد رکھیں کہ ویسے تو اینٹی وائرس کئی میل ویئرز کی شناخت کر سکتاہے اوراُنہیں روک سکتا ہے لیکن حملہ آور ہمیشہ میل ویئر کے نئے ورژنز بنا رہے ہوتے ہیں جنہیں اینٹی وائرس پکڑ نہیں پاتے، نتیجتاً آپ کو اپنے آپ کو محفوظ رکھنے کے لیے صرف اینٹی وائرس پر انحصار نہیں کرنا ہو گا بلکہ آپ کو اس کے لیے کچھ اضافی اقدامات اُٹھانے پڑیں گے۔

سب سے پہلا قدم یہ ہوگا کہ آپ اس بات کا یقین کرلیں کہ آپ کا آپریٹنگ سسٹم اور ایپلیکیشن خود کار طور پر سیکیورٹی اپڈیٹس انسٹال کررہی ہوں- آپ کا سافٹ ویئر جتنا نیا ہوگا اُتنا ہی سائبر مجرمان کے لیے آپ کے کمپیوٹرز اور موبائل آلات کو متاثر کرنا مشکل ہوگا۔

دوسرا قدم یہ ہے کہ آپ اس بات کو یاد رکھیں کہ میل ویئر کے خلاف سب سے بہترین دفاع آپ خود ہیں- میل ویئر کے ذریعے آپ کو متاثر کرنے کے عمل میں اکثر سوشل انجینیئرنگ شامل ہوتی ہے جس کے ذریعے حملہ آور آپ کو ایسے بیوقوف بناتا ہے یا جھانسہ دیتا ہے کہ آپ خود اُس کے لئےمیل ویئر انسٹال کر دیتے ہیں- ایک عام مثال فشنگ اٹیکس کی ہے، یہ وہ ای-میلز ہوتی ہیں جو بظاہر صحیح لگ رہی ہوتی ہیں لیکن حقیقت میں جعلی ہوتی ہیں جو خاص طورپر آپ کو جھانسہ دے کر آپ کے کمپیوٹر کو متاثر کرنے کے لیے بنائی جاتی ہیں۔ مثلاً ایک سائبر مجرم آپ کو آپ کے بینک کے طور پر ای-میل بھیج سکتا ہے یا اور آپ کو ایک لنک کِلک کرنے کا کہہ سکتا ہے- اگر آپ اُس لنک کو کلک کرتے ہیں تو وہ آپ کو ایک

میل ویئر کیا ہے

ایسی ویب سائٹ پر لے جاتا ہے جو خود کار طور پر آپ کے کمپیوٹر کو ہیک اور متاثر کرنے کی کوشش کرتی ہے یا پھر وہ آپ کو ای-میل کے ذریعے نوٹس بھیجتے ہیں کہ آپ کا سامان پہنچایا نہیں جاسکتا ہے اور پھر آپ کو اُس ای-میل سے منسلک ٹریکنگ کی دستاویز کھولنے کا کہتے ہیں جسے اگر آپ کھولیں تو آپ کا کمپیوٹر متاثر ہوجاتاہے۔

سوشل انجینئرنگ کے حملے دوسری ٹیکنالوجیز پر بھی ہوتے ہیں جیسے کہ آپ کا فون- مثال کے طور پر ہیکر مائیکروسافٹ کی ٹیکنیکل سپورٹ ٹیم کا نمائندہ بن کر آپ کو کال کرکے یہ بتا سکتا ہے کہ آپ کا کمپیوٹر متاثر ہوگیا ہے- اُن کی یہ کہانی جھوٹ پر مبنی ہوتی ہے اور اس بات کا قوی امکان ہے کہ آپ کا کمپیوٹر بالکل صحیح ہو- ان کا مقصد آپ کو بیوقوف بناکر اس بات کا یقین دلانا ہے کہ آپ کا کمپیوٹر متاثر ہوچکا ہے اور پھر آپ کو جھانسہ دے کر آپ سے ریموٹ ایکسس لینا ہے یا آپ کو سیکیورٹی سافٹ ویئر بیچنا ہے جو کہ ایک میل ویئر کے علاوہ کچھ نہیں ہوتا- آپ عقل استعمال کریں- اگر آپ کو کوئی فون کال یا میسیج عجیب لگے یا ناقابلِ یقین لگے تو اس بات کا قوی امکان ہے کہ ایسا ہی ہو۔

آخر میں یہ کہ میل ویئر سے دفاع کا بہترین طریقہ اپنے سافٹ ویئر کو اپڈیٹ رکھنا، قابلِ اعتماد ونڈرز سے اینٹی وائرس انسٹال کرنا اور اس بات سے ہوشیار رہنا ہے کہ کوئی بھی آپ کو بیوقوف بناکر یا جھانسہ دے کر آپ کے اپنے کمپیوٹر کو متاثر کرواسکتا ہے۔

مزید جانئے:

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

اردو ایڈیشن

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

وسائل:

OUCH فشنگ:

www.securingthehuman.org/resources/newsletters/ouch/2013#february2013

OUCH اپنے کمپیوٹر کو محفوظ رکھنا:

http://www.securingthehuman.org/resources/newsletters/ouch/2012#december2012

'آپ نشانہ ہیں کا' پوسٹر:

http://www.securingthehuman.org/resources/posters

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

ترجمہ: شعیب ہاشمی