کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- جائزہ
- اینٹی وائیرس کام کیسے کرتا ہے
- اینٹی وائیرس سے متعلق تجاویز

اینٹی وائیرس کیا ہے؟

جائزہ

اینٹی وائیرس ایک سکیورٹی پروگرام ہے جسے آپ اپنے کمپیوٹر یا موبائل آلے پر انسٹال کرتے ہیں میلویئر سے حفاظت کے لیے- 'میلویئر' کی اصطلاح عموماً کسی بھی طرح کے مضر سافٹ ویئر جیسے کہ وائیرس، ورم، ٹراجن، اسپائی ویئر کے لیے استعما ل ہوتی ہے۔ درحقیقت میلویئر کی اصطلاح دو الفاظ 'ملیشئس' اور 'سافٹ ویئر' کے امتزاج سے بنی ہے- اگر آپ کا کمپیوٹر میلویئر سے متاثر ہوچکا ہے تو ایک سائبرحملہ آور آپ کی تمام 'کی اسٹروکس' کو جان سکتا ہے، آپ کی دستاویزات چرا سکتا ہے یا آپ کے کمپیوٹر کو استعمال کرتے ہوئے دوسروں پر حملہ کرسکتا ہے- کچھ لوگوں کی سوچ کے برعکس کوئی بھی آپریٹنگ سسٹم بشمول میکOS Xاور لینکس بھی متاثر ہوسکتا ہیں۔

مہمان ایڈیٹر

جیک ولیمز رینڈیشن انفوسیک (**www.renditioninfosec.com**) کے بانی ہیں اور SANS کے سند یافتہ انسٹرکٹر اور کورس کے مصنف ہیں۔ وہ ٹوئیٹر پر **@MalwareJake** کے ذریعے فعال ہیں اور اپنے بلاگ **malwarejake.blogspot.com** پر لکھتے ہیں۔

آپ اینٹی وائیرس سافٹ ویئر کو ایک علیحدہ حل کے طور پر خرید سکتے ہیں، یہ اکثر سکیورٹی پیکج کا حصہ ہوتا ہے۔ مسئلہ یہ ہے کہ اینٹی وائیرس، سائبرحملہ آوروں کا مقابلہ نہیں کر سکتاہے کیونکہ وہ مسلسل نئی طرح کے میلویئر بنا اور جاری کر رہے ہوتے ہیں۔ روزانہ میلویئر کے اتنے سارے ورژنز جاری ہوتے ہیں کہ کوئی بھی اینٹی وائیرس پروگرام ان سب کی نشاندہی اور ان کے خلاف حفاظت فراہم نہیں کر سکتا ہے۔ اس لیۓ آپ کے لیۓ یہ سمجھنااہم ہے کہ اینٹی وائیرس جبکہ آپ کے کمپیوٹر کی حفاظت کرنے میں مدد فراہم کرتا ہے، یہ تمام قسم کے میلویئر کو پکڑ یا روک نہیں سکتا ہے۔ اس بات کو بہتر طور پر سمجھنے کے لیے ہمیں یہ جاننا ہوگا کہ یہ پروگرام کام کیسے کرتے ہیں۔

اینٹی وائیرس کام کیسے کرتا ہے؟

عموماً اینٹی وائیرس سافٹ ویئر میں میلویئر کو شناخت کرنے کے دو طریقے ہوتے ہیں؛ دستخط کے ذریعے شناخت کرنا اور رویّے کے ذریعے شناخت کرنا۔ دستخط کے ذریعے شناخت بالکل ایسے کام کرتی ہے جیسے کہ ایک انسان کا مدافعتی نظام۔ وہ آپ کے کمپیوٹر کو معروف مضر پروگرامز کی خصوصیات یا دستخط کے لیۓ اسکین کرتا ہے۔ اینٹی وائیرس یہ اسکین معروف میلویئر کی لغت کے ذریعے کرتا ہے، اگر آپ کے کمپیوٹر میں کوئی بھی چیز اس لغت میں موجود نمونے سے مشابہت رکھتی ہے تو یہ پروگرام اُسے بے اثر کرنے کی کوشش کرے گا۔ انسانی مدافعتی نظام کی طرح لغت والے طریقہ کار کو بھی اپڈیٹ کی ضرورت ہوتی ہے، جیسے کہ فلو شاٹس، جو کہ میلویئر کے نئے نقصان سے حفاظت فراہم کرتا ہے۔ اینٹی وائیرس صرف اُس چیز کے خلاف حفاظت فراہم کرتا ہے جسے وہ نقصاندہ تسلیم کرتا ہے مسَلہ یہ ہے کہ سائبر حملہ آور میلویئر اتنی تیزی سے بنا رہے ہیں کہ اینٹی وائیرس ونڈرز کے لئے اُن سب کو روکنا مشکل ہے۔ نتیجتاً آپ کا اینٹی وائیرس چاہے جتنا بھی حال میں اپڈیٹ ہوا ہو، کوئی نہ کوئی میلویئر کا متبادل آپ کے اینٹی وائیرس سافٹ ویئر سے ممکنہ طور پر بچ نکلے گا۔

اینٹی وائیرس کیا ہے؟

اینٹی وائیرس حالانکہ حفاظت کا ایک اہم جز ہے، یہ مکمل طور پر حملوں کی نشاندہی یا اُنہے روک نہیں سکتا ہے۔ بالآخر آپ، نہ کہ ٹیکنالوجی، سب سے بہترین دفاع ہیں۔

رویّے کے ذریعے شناخت میں اینٹی وائیرس معروف میلویئر کو شناخت کرنے کی کوشش نہیں کرتا ہے بلکہ آپ کے کمپیوٹر میں انسٹال سافٹ ویئر کے رویّے کی نگرانی کرتا ہے۔ جب کسی پروگرام کا برتاؤ مشکوک ہو جائے جیسے کہ کسی محفوظ فائل تک رسائی حاصل کرنے کی کوشش کرنا یا کسی دوسرے پروگرام میں تبدیلی کرنا، تو رویّے پر مبنی اینٹی وائیرس سافٹ ویئر اس مشکوک سرگرمی کی نشاندہی کرتا ہے اور آپ کو اُس کے بارے میں ہوشیار کرتا ہے۔ یہ طریقہ کار نئی طرح کے میلویئر، جو کہ کسی بھی لغت میں موجود نہیں ہوتے ہیں، کے خلاف حفاظت فراہم کرتا ہے۔ اس طریقہ کار میں مسئلہ یہ ہے کہ یہ غلط انتباہ بھیج سکتا ہے۔ آپ، یعنی کمپیوٹر کا استعمال کرنے والے، شاید بے یقینی کیفیت سے دوچار ہوں کہ کس چیز کی اجازت دینی ہے یا کس چیز کی اجازت نہیں دینی اور وقت گزرنے کے ساتھ آپ اُن تمام انتباہات کے بارے میں غیر حساس ہو جاتے ہیں۔ آپ شاید ہر 'Accept' کے انتباہ کو کلک کرنا چاہیں جس کے نتیجے میں آپ کے کمپیوٹر پر کوئی بھی حملہ کر سکتا ہے یا اُسے متاثر کر سکتا ہے۔ اس کے علاوہ یہ کہ جب تک اس رویّے کی نشاندہی ہوتی ہے، میلویئر آپ کے کمپیوٹر پر چل چکا ہوتا ہے اور آپ کو شاید یہ پتہ بھی نہیں چلتا کہ اینٹی وائیرس سافٹ ویئر کی شناخت سے پہلے اس میلویئر نے کیا کاروائی کی ہے۔

اینٹی وائیرس آپ کے کمپیوٹر اور موبائل آلات کو محفوظ رکھنے کے لئے ایک اہم جز ہے، ہمارا مشورہ یہ ہے کہ جب بھی ممکن ہو آپ اُسے انسٹال کریں اور فعّال طور پر اس کا استعمال کریں۔ تاہم یاد رکھنے کے لئے سب سے اہم نکتہ یہ ہے کہ اس بات سے قطع نظر کہ اینٹی وائیرس کس طرح کام کرتا ہے، وہ کبھی بھی آپ کو ہر طرح کے میلویئر سے حفاظت فراہم نہیں کر سکتا ہے۔ بالآخر آپ، نہ کہ صرف ٹیکنالوجی، آج کل کے سائبر حملہ آوروں کے خلاف بہترین دفاع ہیں۔

اینٹی وائیرس تجاویز

۱. اینٹی وائیرس سافٹ ویئر کو آپ صرف معروف، قابل اعتماد ذرائع اور وینڈرز سے حاصل کریں۔ سائبر حملہ آوروں کی یہ ایک عام چال ہے کہ وہ جعلی اینٹی وائیرس پروگرامز تقسیم کرتے ہیں جو کہ درحقیقت میلویئر ہوتے ہیں۔

۲. اس بات کا یقین کر لیں کہ آپ کے پاس جو اینٹی وائیرس سافٹ ویئر انسٹال ہے، اُس کا جدید ترین ورژن آپ کے پاس ہے، اور یہ کہ آپ نے سالانہ سبسکرپشن فیس ادا کی ہوئی ہے اور وہ فعّال ہے، اور یہ کہ آپ کا اینٹی وائیرس خودکار اپڈیٹ کے لئے کنفیگر ہے- اگر آپ کا کمپیوٹر آف لائن ہے یا تھوڑی دیر کے لئے بند ہوا ہے تو آپ کے اینٹی وائیرس سافٹ ویئر کو اپڈیٹ کی ضرورت پڑے گی جب آپ اُسے دوبارہ کھلوئیں گے یا انٹر نیٹ سے منسلک کریں گے۔ ان اپڈیٹس کو ملتوی نہیں کریں۔

۳. اس بات کی یقین دہانی کر لیں کہ آپ کا اینٹی وائیرس خود کار طور پر پورٹیبل آلات، جیسے کہ یو ایس بی، کو اسکین کرتا ہے اور اس بات کو بھی یقینی بنائیں کہ حقیقی وقت (Real-time) میں تحفظ کا آپشن فعال ہے-

۴. آپ اپنی اسکرین پر اینٹی وائیرس سافٹ ویئر کی جانب سے بھیجی گئی ہر انتباہ اور الرٹ پر توجہ دیں۔ زیادہ تر الرٹس میں مزید معلومات جاننے یا اگلے اقدامات سے متعلق سفارشات کے اختیارات شامل ہوتے ہیں۔ اگر آپ کو اپنے دفتر کے کمپیوٹر پر کوئی الرٹ ملتا ہے تو وہ آپ اپنے ہیلپ ڈیسک یا سپروائزر سے فوری رابطے کو یقینی بنائیں-

اینٹی وائیرس کیا ہے؟

۵. آپ اپنے اینٹی وائیرس کو اس وجہ سے غیر فعال یا ان انسٹال نہیں کریں کہ آپ کو لگ رہا ہے کہ اسکی وجہ سے آپ کا کمپیوٹر آہستہ ہو رہا ہے، کسی ویب سائٹ کو روک رہا ہے یا آپ کو کسی ایپلیکیشن یا پروگرام کو انسٹال کرنے سے روک رہا ہے۔ اپنے اینٹی وائیرس کو غیر فعّال کرنے سے آپ اپنے آپ کو غیر ضروری خطرے کی طرف دھکیل دیتے ہیں جس کی وجہ سے کوئی بھی سنگین سکیورٹی واقعہ رونما ہو سکتا ہے۔ اگر آپکے دفتر کے کمپیوٹر پر مسائل برقرار رہتے ہیں تو اینٹی وائیرس کمپنی سے رابطہ کرنے کی کوشش کریں، اُن کی ویب سائٹ پر جا کر مزید معلومات حاصل کریں یا اپنے اینٹی وائیرس کو کسی دوسرے اینٹی وائیرس سے تبدیل کر لیں۔

۶. ایک سے زیادہ اینٹی وائیرس پروگرامز اپنے کمپیوٹر میں ایک ہی وقت میں انسٹال نہیں کریں۔ اس طرح کرنے سے ان پروگرامز میں آپس میں تنازع شروع ہو جائے گا اور شاید آپکے کمپیوٹر کی سکیورٹی بھی کم ہو جائے۔

۷. اپنے اینٹی وایئرس سافٹ ویئر کے انتباہ کو پہچاننا سیکھیں۔ سائبرحملہ آور ایسی متاثرہ ویب سائٹس بنا سکتے ہیں جو کہ جعلی اینٹی وائیرس کا بالکل اصلی انتباہ بھیج سکتی ہیں اور آپ کو اپنے کمپیوٹر کو «ٹھیک» کرنے کے لیۓ مدد کی پیشکش بھی کرسکتی ہیں۔ ان ویب سائٹس پر موجود لنکس یا بٹن کوکلک کرنے سے در حقیقت آپکے کمپیوٹر کو نقصان پہنچ سکتا ہے۔

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 لیۓ 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:

اینٹی وائرس مصنوعات کا موازنہ: http://www.av-test.org/en/

سوشل انجینیئرنگ: http://www.securingthehuman.org/ouch/2014#november2014

ای میل فشنگ حملے: http://www.securingthehuman.org/ouch/2013#february2013

میں ہیک ہوچکا ہوں، اب؟: http://www.securingthehuman.org/ouch/2014#may2014

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

ترجمہ: شعیب ہاشمی