کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سیکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- جائزہ
- ہیک ہونے کے آثار
- ردِ عمل کیسے ظاہر کرنا ہے

میں ہیک ہوچکا ہوں، اب؟

جائزہ

ہم جانتے ہیں کہ آپ اپنے کمپیوٹر اور معلومات کو محفوظ رکھنے کیلئے فکر مند رہتے ہیں اور اس سلسلے میں اقدامات بھی کرتے ہیں تاہم، یہ بالکل گاڑی چلانے کے مترادف ہے، یعنی آپ جتنی بھی محفوظ گاڑی چلالیں کبھی نہ کبھی آپ کے ساتھ کوئی واقعہ پیش آسکتا ہے- اس شمارے میں ہم آپ کو یہ سکھائیں گے کہ آپ کس طرح اس بات کا تعین کریں کہ آپ کا کمپیوٹر ہیک ہوگیا ہے۔ اور اگر ہوگیا ہے تو آپ کو کیا کرنا چاہیے- بلآخر آپ جتنی جلدی اپنے کمپیوٹر کے ہیک ہونے کی نشاندہی کریں گے اور اُس کا جتنا جلدی مثبت جواب دیں گے، اتنا ہی بہتر طریقے سے آپ اپنے آپ یا اپنی تنظیم کو کسی بھی نقصان سے بچا سکتے ہیں۔

مہمان ایڈیٹر

جیک ولیمز(Malwarejake.blogspot.com ;@MalwareJake)سی ایس آر گروپ کمپیوٹر سیکیورٹی کنسلٹینٹس میں چیف سائنسدان ہیں۔ وہ SANS میں میموری فوریزنک (FOR526)اور میلویئر ریورس انجینیئرنگ (FOR610)کورسز کے شریک مصنف بھی ہیں-

ہیک ہونے کے آثار:

سب سے پہلے آپ کو یہ سمجھنے کی ضرورت ہے کہ کئی صورتوں میں آپ کوئی بھی ایک ایسا قدم نہیں اُٹھا سکتے ہیں جس کے ذریعے آپ اپنے کمپیوٹر کے ہیک ہونے کا تعین کرسکیں- اس کے بجائے عام طور پر اس کی کئی اور نشانیاں ہیں- اگر آپ ان سب نشانیوں کی مجموعی طور پر شناخت کرتے ہیں تو اس کا مطلب ہے کہ آپ کا کمپیوٹر ہیک ہوچکا ہے۔ چند مثالیں یہ ہیں:

- آپ کے اینٹی وائرس پروگرام نے آپ کو ایک آلرٹ بھیجا ہے کہ آپ کا کمپیوٹر متاثر ہوگیا ہے۔ خاص طور پر اس وقت جب وہ یہ کہے کہ وہ متاثرہ فائلز کو ہٹانے یاالگ کرنے (Quarantine) سے قاصر ہے۔
- آپ کے براؤزر کا ہوم پیج غیر متوقع طور پر تبدیل ہوگیا ہے یا آپ کا براؤزر آپ کو ایسی ویب سائٹس پر لے جارہا ہے جہاں آپ جانا نہیں چاہتے ہیں۔
- آپ کے کمپیوٹر پر نئے آکاؤنٹس بن گئے ہیں جو آپ نے نہیں بنائے ہیں۔
- آپ کے کمپیوٹر پر ایسے نئے پروگرامز چل رہے ہیں جنہیں آپ نے انسٹال نہیں کیا ہے۔
- آپ کا کمپیوٹر مسلسل کریش ہورہا ہے یا بہت آہستہ چل رہا ہے۔
- آپ کے کمپیوٹر پر ایک پروگرام آپ سے سسٹم میں کچھ تبدیلیاں کرنے کیلئے اجازت مانگ رہا ہے حالانکہ آپ ابھی کوئی بھی ایپلیکیشن انسٹال یا اپڈیٹ نہیں کررہے ہیں ۔
- آپ کا فائروآل آپ کو الرٹ بھیجتا ہے کہ ایک نامعلوم پروگرام انٹرنیٹ پر رسائی کیلئے اجازت مانگ رہا ہے۔

میں ہیک ہوچکا ہوں، اب؟

ردِ عمل کیسے ظاہر کرنا ہے:

اگر آپ سمجھتے ہے کہ آپ کا کمپیوٹر ہیک ہوگیا ہے تو آپ جتنا جلدی اس کا ردِ عمل ظاہر کریں گے اتنا ہی بہتر ہوگا۔ اگر آپ کے زیرِ استعمال کمپیوٹر آپ کے آجر کی طرف سے مہیا کیا گیا ہے یا وہ دفتر کے کام کیلئے استعمال ہوتا ہے تو آپ خود اسے صحیح نہیں کریں اور نہ ہی اسے بند کریں۔ آپ نہ صرف اسے صحیح کرنے کے بجائے مزید نقصان پہنچائیں گے بلکہ آپ اہم ثبوت کو تباہ کرسکتے ہیں جو کہ تفتیش کیلئے استعمال ہوسکتا ہے۔ اس کے بجائے آپ ہیلپ ڈیسک، سیکیورٹی ٹیم یا سپروائزر سے رجوع کرکے واقعہ کے بارے میں فوراً اپنے آجر کو بتائیں ۔ اگر آپ کسی بھی وجہ سے اپنی تنظیم سے رجوع نہیں کرسکتے ہیں یا تاخیر ہونے کے بارے میں فکر مند ہیں تو آپ اپنے کمپیوٹر کو نیٹ ورک سے منقطع کردیں اور پھر اسے سلیپ، سسپینڈ یا ہائیبرنیشن موڈ میں ڈال دیں۔ اگر آپ کو اس بات کا یقین نہیں ہے کہ آپ ہیک ہوگئے ہیں پھر بھی احتیاطاً اس واقعہ کو رپورٹ کرنا بہتر ہے۔ اس بات کا زیادہ امکان ہے کہ آپ کی تنظیم کے پاس اس صورتحال سے نمٹنے کیلئے کچھ اقدامات اور ایک ٹیم ہو، آپ انہیں اسے سنبھالنے دیں۔

آج یا کل آپ کا کمپیوٹر ہیک ہوسکتا ہے اس لیے آپ جتنا جلدی کسی واقعے کا پتہ لگاتے ہیں اور اس کا جواب دیتے ہیں، اتنا ہی بہتر ہوتا ہے۔

اگر کمپیوٹر آپ کا اپنا ہے اور ذاتی استعمال میں ہے تو آ پ اپنے طور پر مندرجہ ذیل اقدامات اٹھا سکتے ہیں:

- **بیک اپ:** سب سے اہم قدم یہ ہوگا کہ آپ بیک اپ کے ذریعے وقت سے پہلے تیار ہوجائیں- اپنی معلومات کا خصوصاً باقاعدگی سے بیک اپ لیں اور گاہے بہ گاہے بیک اپ سے فائلز کو ری اسٹور کرکے دیکھتے رہیں- اکثر جب کمپیوٹر ہیک ہوتا ہے تو جو اختیار آپ کے پاس رہ جاتا ہے وہ آیا سسٹم کی ہارڈڈسک کا صفایا اور آپریٹنگ سسٹم کو پھر سے انسٹال کرنا یا پھر نیا کمپیوٹر خریدنا ہوتا ہے۔ دونوں صورتوں میں آپ کو اپنی ذاتی معلومات بیک اپ کے ذریعے بحال کرنے کی ضرورت ہوتی ہے۔
- **اپنے پاسورڈ کو تبدیل کردیں:** آپ اس بات کا یقین کرلیں کہ آپ نے تمام پاسورڈ ز تبدیل کردیئے ہیں- اس میں نہ صرف آپ کے کمپیوٹر اور موبائل ڈیوائیسز کے پاسورڈ شامل ہیں بلکہ آپ کے تمام آن لائن پاسورڈ ز شامل ہیں- آپ اس بات کا یقین کرلیں کہ آپ نے اپنے تمام آن لائن پاسورڈ ز کسی ایسے کمپیوٹر کے ذریعے تبدیل کئے ہیں جو آپ کے خیال میں قابلِ اعتماد اور محفوظ ہیں۔
- **اینٹی وائرس:** اگر آپ کا اینٹی وائرس سافٹ ویئر آپ کو کسی فائل کے متاثر ہونے کی اطلاع دیتا ہے تو آپ اس کی دی ہوئی سفارشات کے مطابق اقدامات کرسکتے ہیں- ان میں فائل کو الگ کرنا(Quarantine)، صاف کرنا یا ڈیلیٹ کرنا شامل ہے۔ کئی اینٹی وائرس سافٹ ویئر ایسے لنکس فراہم کرتے ہیں جن ذریعے آپ مخصوص انفیکشن کے بارے میں مزید جان سکتے ہیں۔ آپ کو جب بھی شک ہو آپ فائل کو الگ (Quarantine) کردیں۔
- **دوبارہ انسٹال کرنا:** اگر آپ اپنے کمپیوٹر کو اینٹی وائرس کے ذریعے صاف کرنے سے قاصر ہیں تو محفوظ ترین طریقوں میں سے ایک یہ ہے کہ آپ اپنے کمپیوٹر کو بالکل شروع سے بنائیں- پہلے آپ اپنے کمپیوٹر کو نیٹ ورک سے منقطع کریں، پھر اپنے سسٹم کے مینوفیکچرر کی ہدایات پر عمل کریں، زیادہ تر صورتوں میں اس کا مطلب پہلے سے بنی ہوئی ریکوری پارٹیشن کو دوبارہ انسٹال کرنا ہوتا ہے۔ اگر

میں ہیک ہوچکا ہوں، اب؟

ریکوڑی پارٹیشن لاپتہ ہوجائے، خراب ہوجائے یا متاثر ہوجائے تو آپ اپنے مینوفیکچرر سے رابطہ کریں اور ان سے ریکوری ڈی وی ڈی بھیجنے کی درخواست کریں- آپ بیک اپ کے ذریعے آپریٹنگ سسٹم کو دوبارہ انسٹال نہیں کریں کیونکہ ہوسکتا ہے کہ آپ کے بیک اپ کو وہی خطرات لاحق ہوں جن کے ذریعے ہیکرز اصل میں اس تک رسائی حاصل کی ہے۔ اپنے بیک اپ کو آپ صرف ذاتی معلومات ریکوڑ کرنے کیلئے استعمال کریں- اس کے علاوہ اگر آپ کا کمپیوٹر پرانا یا فرسودہ ہوچکا ہے تو نیا کمپیوٹر خریدنا زیادہ بہتر ہوگا اور شاید سستا بھی بنسبت اپنے کمپیوٹر کو کئی گھنٹے لگا کر پھر سے بنانے سے۔

- **پیشہ ورانہ مدد:** اگر آپ کو اس بات کی تشویش ہے کہ آپ ہیک ہوگئے ہیں لیکن آپ سمجھتے ہیں کہ آپ کے پاس اسے صحیح کرنے کیلئے مہارت اور علم نہیں ہے تو آپ کو اپنے کمپیوٹر کو کسی پیشہ ور آدمی کو دکھانا چاہیے ، مثال کے طور پر ہیک ہونے کے بعد آپ کو لگ رہا ہے کہ آپ کا بیک اپ نا مکمل یا پرانا ہے- شاید آپ اپنی نئی اور متاثرہ مشین کے درمیان اہم فائلز جیسے کہ تصاویر ، دستاویزات یا ویڈیوز کی منتقلی کیلئے کچھ بیتاب ہوں لیکن ایسا کرنے کی صورت میں آپ غیر دانستہ طور پر اپنے نئے کمپیوٹر میں میل ویئر منتقل کرسکتے ہیں۔ اس سے کہیں زیادہ محفوظ متبادل راستہ یہ ہوگا کہ آپ متاثرہ کمپیوٹر کو کسی ایسے قابل ٹیکنیشن کے پاس لے جائیں جو باحفاظت فائلز کو میل ویئر منتقل کئے بغیر ریکوڑ کردے۔

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 یاہمارے فیس بک پیج https://www.facebook.com/Rewterz کو 'Like' کریں یا ٹوئیٹر @Rewterz پر فالو کریں۔

وسائل:

OUCH! بیک اپس:	http://www.securingthehuman.org/ouch/2013#september2013
OUCH! پاس ورڈز:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! میل ویئر کیا ہے:	http://www.securingthehuman.org/ouch/2014#february2014
"برائی کی شناخت" کا پوسٹر:	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

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

ترجمہ: شعیب ہاشمی