تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

OUCH!

اس شمارے میں شامل ہے:

- پس منظر
- پیچنگ
- بیک اپس
- فشنگ

WannaCry سے ہمیں کیا سبق ملا

جائزہ

حال ہی میں آپ نے ایک سائبر حملے "WannaCry" کے بارے میں خبروں میں کافی سنا ہو گا- "WannaCry" نے ۲ لاکھ سے زائد کمپیوٹرز کو متاثر کیا ہے جس کی وجہ سے کئی تنظیموں، جن میں بریطانیہ کے ہسپتال بھی شامل ہیں، کو اپنی معلومات سے محروُم ہونا پڑا ہے- اس حملے کو اتنی توجّہ ملنے کی کئی وجوہات ہیں- پہلی بات یہ کہ یہ میلویئر وِنڈوز کمپیوٹرز میں موجود ایک معروف کمزوری کے ذریعے ایک کمپیوٹر سے دوسرے کمپیوٹر میں پھیلتا ہے- دوسری بات یہ ہے کہ یہ حملہ ایک طرح کا میلویئر ہے جو کہ «رینسمویئر» کہلاتا ہے جس کا مطلب ہے کہ ایک بار اگر یہ آپ کے کمپیوٹر کو متاثر کر دیتا ہے تو اس میں موجود تمام فائلز انکرپٹ ہو جاتی ہیں جس کی وجہ سے آپ اپنی تمام معلومات سے دُور ہو جاتے ہیں- اپنی معلومات کو ریکوَر کرنے کا واحد طریقہ بیک اپس کے ذریعے ہے ورنہ دوسری صورت میں آپ کو حملہ آور کو اپنی معلومات کو ڈیکرپٹ کرنے کے لیئے ۳۰۰ ڈالر کا تاوان دینا پڑے گا- تیسری اور سب سے اہم بات یہ ہے کہ یہ حملہ کبھی ہونا ہی نہیں چاہیئے تھا- "WannaCry" وِنڈوز کمپیوٹرز میں جس کمزوری کا فائدہ اُٹھا کر حملہ کر رہا تھا اُس کے بارے میں مائیکروسافٹ کو اچھی طرح سے علم تھا اور اُس نے چند مہینوں پہلے ہی اس کا پیچ بھی جاری کیا تھا- لیکن کئی تنظیموں نے اس پیچ کو انسٹال نہیں کیا یا وہ وِنڈوز ایکس پی جیسے آپریٹنگ سسٹمز استعمال کر رہے تھے جو کہ بہت پُرانے ہو چکے ہیں اور اُن کا کوئی پیچ اب موجود بھی نہیں ہے- آپ مندرجہ ذیل تین آسان اقدامات اُٹھا کر WannaCryجیسے میلویئر سے اپنے آپ کو ہمیشہ بچا سکتے ہیں-

مہمان ایڈیٹر

ڈاکٹر جوہینس اُلرچ SANS ٹیکنالوجی انسٹیٹیوٹ میں تحقیق کے ڈین اور DShield.org کے بانی ہیں- وہ **SANS انٹرنیٹ اسٹورم سینٹر** کے بھی ذمہ دار ہیں جو کہ موجودہ سائبر سکیورٹی خطرات کی نگرانی کرتا ہے- وہ ویب ایپلیکیشن سکیورٹی (**DEV522**)، اِنٹرُوژن ڈیٹیکشن (**SEC503**) اور IPv6 (**SEC546**) کے کورسز پڑھاتے ہیں-

پیچنگ

سب سے پہلی اور اہم بات یہ ہے کہ آپ اس بات کی یقین دہانی کر لیں کہ آپ کے تمام کمپیوٹرز، موبائل آلات، ایپلیکیشنز اور انٹرنیٹ سے مُنسلک ہونے والے کسی بھی آلہ میں سافٹ ویئر کا جدید ترین ورژن انسٹال ہوا ہو- سائبر مجرمان ہمیشہ آپ کے آلات کے سافٹ ویئر میں نئی کمزوریوں کی تلاش میں ہوتے ہیں- آپ کے زیراستعمال آلات میں جب بھی اُنہیں کمزوریاں نظر آتی ہیں تو وہ خاص پروگرامز کے ذریعے اُن کو ہیک کر لیتے ہیں- دریں اثناء وہ تنظیمیں جو آپ کے آلات کے لیئے سافٹ ویئر تخلیق کرتی ہیں، وہ ان کمزوریوں کو درست کرنے کے لیئے کافی محنت کے بعد اپڈیٹس جاری کرتی ہیں- آپ اس بات کو یقینی بنا کر کہ آپ کے کمپیوٹرز اور موبائل آلات میں یہ اپڈیٹس انسٹال ہیں، کسی کے لیئے بھی اس کا ہیک کرنا کافی مشکل بنا دیتے ہیں- یہی بات WannaCry کے پھیلاؤ سے متعلق کافی پریشان کُن ہے- اس حملے سے بچاؤ کے لیئے مائیکروسافٹ نے دو مہینے پہلے ہی اپڈیٹس جاری کی تھیں- اگر تنظیموں نے اپنے کمپیوٹرز کو اپڈیٹ رکھا ہوتا تو یہ حملہ کبھی بھی کامیاب نہیں ہوتا- اس بات کو یقینی بنانے کے لیئے کہ آپ کے آلات میں تازہ ترین

WannaCry سے ہمیں کیا سبق ملا

اپڈیٹس موجود ہیں، آپ جب بھی مُمکن ہو اُن میں خودکار اپڈیٹس کو فعّال کر دیں- یہ اصول نیٹ ورک سے مُنسلک ہونے والی تقریباً ہر ٹیکنالوجی پر لاگو ہوتا ہے، نہ صرف کمپیوٹرز یا موبائل آلات پر بلکہ انٹرنیٹ سے مُنسلک ٹی وی، گھر کے راؤٹرز، گیمنگ کنسولز یا ایک دن شاید آپ کی گاڑی بھی اس میں شامل ہو- اگر آپ کے آپریٹنگ سسٹمز یا آلات اتنے پُرانے ہو گئے ہیں کہ اُن میں سکیورٹی اپڈیٹس کی حمات باقی نہیں رہی، جیسے کہ وِنڈوز ایکس پی میں، تو آپ اُنہیں اس نئے آپریٹنگ سسٹم یا آلہ سے تبدیل کر دیں جس میں سکیورٹی اپڈیٹس کی حمایت ہو-

اپنے آپ کو WannaCry جیسے حملوں سے بچانے کے لیئے تین آسان اقدامات اُٹھایں؛ اپنے کمپیوٹرز کو اپڈیٹ رکھیں، فشنگ حملوں سے ہوشیار رہیں اور اپنے سسٹمز کا بیک اپ لیتے رہیں-

بیک اپس

کُچھ صورتوں میں جیسے کہ رینسمویئر جیسے سائبر حملوں میں اپڈیٹڈ سسٹمز بھی متاثر ہو سکتے ہیں- اپنے آپ کو محفوظ رکھنے کا ایک اور طریقہ اپنی معلومات کا بیک اپ لینا ہے- بیک اپس آپ کی معلومات کی ایسی نقل ہوتے ہیں جو کہ کمپیوٹر یا موبائل آلات کے علاوہ کسی دوسری جگہ پر ذخیرہ ہوتے ہیں- جب آپ قیمتی معلومات کھو دیتے ہیں تو آپ اُنہیں بیک اپس کے ذریعے بازیاب کروا سکتے ہیں- بد قسمتی سے لوگوں کی اکثریت باقاعدگی سے بیک اپ نہیں لیتی ہے، حالانکہ یہ بہت آسان اور سستا طریقہ ہے- اپنی معلومات کا بیک اپ لینے کے دو طریقے ہیں: فزیکل میڈیا یا کلاؤڈ پر مُنحصر اسٹوریج- دونوں طریقوں میں کُچھ فائدے اور نقصانات ہیں- اگر آپ کسی ایک طریقہ کار کے استعمال سے متعلق بے یقینی کا شکار ہیں تو آپ دونوں طریقوں کا ایک ساتھ استعمال کر سکتے ہیں-

فزیکل میڈیا وہ آلات ہوتے ہیں جن پر آپ کو اختیار حاصل ہوتا ہے جیسے کہ یوایس بی ڈرائیوز یا آپ کے گھر یا دفتر میں نیٹ ورک سے مُنسلک ڈرائیوز- اپنی ذاتی فزیکل میڈیا استعمال کرنے کا فائدہ یہ ہے کہ آپ اس کے ذریعے بڑی مقدار میں معلومات کو بہت تیزی کے ساتھ بیک اپ اور ریکوَر کر سکتے ہیں- اس طریقہ کار میں نقصان یہ ہے کہ اگر رینسمویئر جیسے میلویئر سے آپ متاثر ہو جائیں تو مُمکن ہے کہ یہ آپ کے بیک اپس کو بھی متاثر کر دے- اگر آپ بیک اپس کے لیئے فزیکل میڈیا کا استعمال کر رہے ہیں تو آپ کو بیک اپ کی نقل کو کسی دوسری محفوظ جگہ پر ذخیرہ کرنا چاہیئے- آپ اس بات کی یقین دہانی کر لیں کہ جس بیک اپ کو آپ ذخیرہ کر رہے ہیں اُس پر باقاعدہ عنوان لکھا ہوا ہے- کلاؤڈ پر مُنحصر سولیوشنز، آن لائن سروسز ہوتی ہیں جو آپ کی فائلز کا بیک اپ اور اُنہیں ذخیرہ انٹرنیٹ پر کرتی ہیں- عام طور پر آپ اپنے کمپیوٹر میں ایک پروگرام انسٹال کرتے ہیں جو ان سب چیزوں کا خیال رکھتا ہے- کلاؤڈ سولیوشنز کا فائدہ یہ ہے کہ یہ بہت آسان ہوتے ہیں- اس کے علاوہ یہ کہ اگر آپ رینسمویئر سے متاثر ہو بھی جاتے ہیں تو عموماً اس سے آپ کے کلاؤڈ پر موجود بیک اپس پر بالکل بھی فرق نہیں پڑتا- نُقصان یہ ہے کہ زیادہ مقدار میں معلومات کا بیک اپ لینے یا اُسے ریکوَر کرنے میں کافی زیادہ وقت لگ سکتا ہے- آپ اس بات کو یقینی بنائیں کہ آپ نے کلاؤڈ بیک اپس کی پرائیویسی اور سکیورٹی پر تحقیق کر لی ہے کہ آیا بیک اپ سروس پرووائیڈر کے پاس مضبوُط سکیورٹی اقدامات جیسے کہ معلومات کو انکرپٹ کرنا اور مضبوط اوتھنٹیکیشن موجود ہے؟

WannaCry سے ہمیں کیا سبق ملا

فشنگ

آخری بات یہ کہ بُرے لوگ ہمیشہ اپنے حملے کے طریقہ کار کو تبدیل کرتے رہتے ہیں- سائبر مجرمان اکثر اپنے اہدف پر حملہ کرنے اور انہیں متاثر کے لیئے ایک طریقہ استعمال کرتے ہیں جو کہ فشنگ کہلاتا ہے- فشنگ میں سائبر مجرمان آپ کو ای میل کے ذریعے جھانسا دے کر اٹیچمنٹ کُھلواتے ہیں یا کسی مُضر ویب سائٹ کے لنک پر جانے کا کہتے ہیں- اگر آپ ان دونوں میں سے کچھ بھی کرتے ہیں تو آپ کا کمپیوٹر متاثر ہو سکتا ہے- WannaCry نے حالانکہ یہ طریقہ استعمال نہیں کیا تھا لیکن عام طور پر یہ دوسری اقسام کے حملوں میں استعمال ہوتا ہے جس میں رینسمویئر کی اقسام بھی شامل ہیں- مزید یہ کہ جن سائبر مجرمان نے WannaCry تخلیق کیا ہے، وہ لازماً آنے والے مہینوں میں حملے کے اس طریقے کو اپڈیٹ کریں گے اور نئی تکنیک جیسے کہ فشنگ کے ذریعے مزید کمپیوٹرز کو متاثر کریں گے- ای میل کے ذریعے ہونے والے حملوں سے بچنے کا سب سے آسان طریقہ اپنے عام فہم کا استعمال کرنا ہے- اگر کوئی ای میل یا پیغام عجیب لگ رہا ہو، مشکوک لگ رہا ہو یا اُس کا سچ ہونا محال ہو تو اس بات کا قوی امکان ہے کہ یہ ایک حملہ ہو-

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 securingthehuman.sans.org/ouch/archives (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:

میلویئر کیا ہے؟:	https://securingthehuman.sans.org/ouch/2016#march2016
رینسمویئر:	https://securingthehuman.sans.org/ouch/2016#august2016
بیک اپس:	https://securingthehuman.sans.org/ouch/2015#august2015
فشنگ:	https://securingthehuman.sans.org/ouch/2015#december2015
کلاؤڈ کا محفوظ طریقے سے استعمال:	https://securingthehuman.sans.org/ouch/2016#november2016

ایڈیٹوریل بورڈ: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley۔

ترجمہ: شعیب ہاشمی