تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

OUCH!

اس شمارے میں شامل ہے:

- رینسم ویئرکیا ہے؟
- کیا آپ کو تاوان دینا چاہیئے؟
- بیک اپس
- مزید حفاظتی اقدامات

رینسم ویئر

رینسم ویئر کیا ہے؟

رینسم ویئر ایک خاص قسم کا میلویئر ہے جو کہ بہت ہی فعّال طریقے سے آج کل پورے انٹرنیٹ پر پھیل رہا ہے۔ یہ میلویئر اپنے شکار کو اس کی دستاویزات اور دوسری فائلز تباہ کرنے کی دھمکی دیتا ہے- میلویئر ایک سافٹ ویئر، ایک کمپیوٹر پروگرام ہوتا ہےجو کہ مضر اقدامات اٹھانے کے لیئے استعمال ہوتا ہے- رینسم ویئرحالانکہ میلویئر کی مختلف اقسام میں سےایک ہے مگر یہ بہت زیادہ عام ہو گیا ہے کیونکہ یہ مجرمان کے لیئے بہت زیادہ منافع بخش ہے۔ ایک بار رینسم ویئرآپ کے کمپیوٹر کو متاثر کر دے تو وہ کچھ فائلز یا مکمل ہارڈ ڈرائیو کو انکرپٹ کر دیتا ہے۔ پھر آپ کا مکمل سسٹم لاک ہو جاتا ہے یا آپ اپنی اہم فائلز جیسے کہ دستاویزات یا تصاویر تک رسائی حاصل نہیں کر سکتے ہیں۔ پھر یہ میلویئر آپ کو مطلع کرتا ہے کہ آپ کی فائلز کو ڈیکرپٹ کرنے اور ان تک دوبارہ رسائی کا واحد راستہ سائبر مجرم کو تاوان دینا ہے (اس لیئے اس کا نام رینسم ویئر ہے)۔ زیادہ تر تاوان کسی ڈیجیٹل کرنسی کی شکل میں دیئے جاتے ہیں جیسے کہ بِٹ کوائن۔ رینسم ویئر بھی کئی دوسری اقسام کے میلویئر کی طرح پھیلتا ہے- مجرمان کے لیئے سب سے عام طریقہ اپنے احداف کو متاثرہ ای-میلز بھیجنا ہے- پھر وہ آپ سے دھوکہ دہی کے ذریعے متاثرہ ای-میل اٹیچمنٹ کھلواتے ہیں یا متاثرہ لنک پر کلک کرواتے ہیں جو کہ آپ کو اس حملہ آور کی ویب سائٹ پر لے جاتا ہے-

مہمان ایڈیٹر

لینی زیلٹسر NCR Corp میں اپنی توجہ صارفین کے ITآپریشنز کی حفاظت پر مرکوز رکھتے ہیں اور SANSانسٹیٹیوٹ میں میلویئر سے نمٹنے سے متعلق تعلیم دیتے ہیں۔ لینی ٹوئیٹر پر **@lennyzeltser** کے ذریعے موجود ہوتے ہیں اور **zeltser.com** پر سکیورٹی بلاگ لکھتے ہیں-

کیا آپ کو تاوان دینا چاہیئے؟

یہ ایک مشکل سوال ہے، مسئلہ یہ ہے کہ اس میلویئر سے متاثرہ لوگ جب تک ان مجرمان کو پیسے دیتے رہیں گے ان کی اتنی ہی حوصلہ افزائی ہوتی رہے گی اور وہ مزید لوگوں کو متاثر کرتے رہیں گے۔ دوسری جانب اپنی فائلز تک دوبارہ رسائی حاصل کرنے کے لیئے ہو سکتا ہے کہ آپ کے پاس کوئی اور راستہ نہیں ہو۔ آپ اس بات سے ہوشیار رہیں کہ اس بات کی کوئی ضمانت نہیں ہے کہ تاوان دینے کے باوجود آپ کو اپنی فائلز واپس مل جائیں گی۔ یہاں آپ مجرمان سے نمٹ رہے ہیں اس لیئے ہو سکتا ہے کہ انھوں نے فائلز ڈی کرپٹ کی ہی نہ ہوں یا وہ پیسے کی ادائیگی کے بدلے میں اگر آپ کو ڈیکرپشن کا طریقہ بتا بھی دیتے ہیں تو ہو سکتا ہے کہ اس عمل کے دوران کچھ غلط ہو جائے یا آپ کا کمپیوٹر دوبارہ کسی میلویئر سے متاثر ہو جائے-

اپنی فائلز کو بیک اپ کریں

رینسم ویئر انفیکشن سے ریکوئر کرنے اور تاوان نہ دینے کا سب سے بہترین طریقہ اپنی فائلز کو بیک اپ کے ذریعے ریکوئر کرنا ہے- اس طرح اگر آپ رینسم ویئر سے متاثر ہو بھی جاتے ہیں تو آپ کے پاس فائلز کو ‹ری بِلڈ› کر کے ریکوئر کرنے یا اپنے کمپیوٹر کو میلویئر سے پاک کرنے کا طریقہ موجود ہوتا ہے- آپ اس بات کو ذہن نشین کر لیں کہ اگر آپ کے بیک اپ تک کسی متاثرہ سسٹم کو رسائی حاصل ہوتی ہے تو ہو سکتا ہے کہ رینسم ویئر

رینسم ویئر

بیک اپ فائلز کو ڈیلیٹ یا انکرپیٹ کر دے- اس لیئے ضروری ہے کہ آپ فائلز کو کسی قابل بھروسہ کلاؤڈ سروس کے ذریعے بیک اپ کریں یا اپنے بیک اپ کو ایسی بیرونی ڈرائیوز پر ذخیرہ کریں جو آپ کے سسٹم سے ہمیشہ منسلک نہیں ہوتی ہوں- مزید یہ کہ ایک عام غلطی جو کہ لوگ بیک اپ کے ساتھ کرتے ہیں وہ یہ ہے کہ لوگ بیک اپس کو ٹیسٹ کیئے بغیر سمجھتے ہیں کہ وہ فائلز ریکوِر کر سکتے ہیں- آپ اس بات کو یقینی بنائیں کہ آپ بیک اپس کو باقائدگی سے ٹیسٹ کرکے دیکھتے رہیں کہ وہ صحیح کام کر رہے ہیں اور اس بات کی بھی تصدیق کر لیں کہ رینسم ویئر سے متاثر ہونے کی صورت میں آپ ضروری فائلز کو ریکوِر کر سکتے ہیں- بیک اپس اہم ہوتے ہیں کیونکہ وہ آپ کو حادثاتی طور پر ڈیلیٹ ہوئی ہوئی فائلز یا ہارڈ ڈرائیو کریش ہونے کی صورت میں آپ کو اسے ریکوِر کرنے میں مدد فراہم کرتے ہیں-

رینسم ویئر ایک میلویئر ہے جس سے اگر ایک بار کمپیوٹر متاثر ہو جائے تو وہ اُس میں موجود تمام فائلز کو انکرپیٹ کر دیتا ہے جس سے آپ کی اُن فائلز تک رسائی ختم ہو جاتی ہے-

مزید حفاظتی اقدامات

آپ اپنے آپ کو رینسم ویئر انفیکشن سے اسی طرح بچا سکتے ہیں جس طرح کسی بھی دوسرے میلویئر سے تاکہ وہ آپ پر اثرانداز نہ ہو- آپ اس کی شروعات اس بات کی یقین دہانی سے کر سکتے ہیں کہ آپ کے پاس کسی قابل بھروسہ وینڈر کا اپڈیٹڈ اینٹی وائرس سافٹ ویئر ہے- اس طرح کے ٹوُلز جو کہ اینٹی میلویئر سافٹ ویئر بھی کہلاتے ہیں، خاص طور پر میلویئر کی تشخیص اور اسے روکنے کے لیئے بنائے جاتے ہیں- تاہم اینٹی وائرس تمام مُضر پروگرامز کو روک یا اُس کا مُکمّل صفایا نہیں کر سکتا ہے- سائبر مجرمان مُسلسل جِدّت لا رہے ہیں اور ایسے نئے اور زیادہ پیچیدہ میلویئر تخلیق کر رہے ہیں جو کسی بھی طرح کی تشخیص سے بچ سکتے ہیں- اس کی وجہ سے اینٹی وائرس وینڈرز کو مُسلسل اپنی مصنوعات کو میلویئر کی تشخیص کے لیئے نئی صلاحیات سے لیس کرنا پڑتا ہے- یہ کئی طرح سے اسلحے کی دوڑ بن گئی ہے جہاں دونوں فریقین ایک دوسرے کو نیچا دکھانے کی کوشش کر رہی ہوتی ہیں- بد قسمتی سے بُرے لوگ اکثر ایک قدم آگے ہی ہوتے ہیں جس کی وجہ سے آپ کے لیئے ضروری ہے کہ آپ اپنی فائلز کا بیک اپ لیں اور مُندرجہ ذیل اضافی اقدامات کو اپنا کر اپنی حفاظت کریں-

- سائبر مجرمان اکثر آپ کے سافٹ ویئر میں موجود کمزوریوں کا فائدہ اٹھاتے ہوئے کمپیوٹرز یا آلات کو متاثر کر دیتے ہیں- آپ کا سافٹ ویئر جتنا حالیہ ہوگا اتنی ہی کم معروف کمزوریاں آپ کے سسٹم میں ہوں گی اور سائبر مجرمان کے لیئے انہیں متاثر کرنا اتنا ہی مشکل ہوگا- اس لیئے آپ اس بات کو یقینی بنائیں کہ آپ نے آپریٹنگ سسٹمز، ایپلیکیشنز اور آلات میں خودکار اپڈیٹس انسٹال کرنے کی خصوصیت کو فعال کر دیا ہے-
- کمپیوٹرز میں آپ ایک اسٹینڈرڈ اکاؤنٹ کا استعمال کریں جس میں محدود اختیارات ہوں نہ کہ زیادہ اختیارات والے اکاؤنٹس جیسے کہ «ایڈمنسٹریٹر» یا «رُوٹ»- یہ قدم کئی اقسام کے میلویئر کو خوُد بخوُد انسٹال ہونے سے بچانے کے لیئے اضافی تحفّظ فراہم کرتا ہے-
- سائبر مُجرمان اکثر لوگوں کو دھوکہ دہی کے ذریعے میلویئر انسٹال کروا دیتے ہیں- مثال کے طور پر وہ آپ کو ایسی ای میل بھیج سکتے ہیں جو کہ دیکھنے میں بالکل صحیح لگتی ہو اور اس میں ایک اٹیچمنٹ یا لنک ہو اور بظاہر ایسا لگتا ہو کہ یہ ای میل آپ کے بینک یا کسی

رینسم ویئر

دوست کی جانب سے آئی ہو- تاہم اگر آپ وہ اٹیچمنٹ کھولیں یا اُس لنک پر کلک کریں تو آپ کسی مُضر کوڈ کو فعّال کر دیں گے جو کہ آپ کے سسٹم میں میلویئر انسٹال کر دے گا- اگر کوئی ای میل پیغام آپ کو عُجلت کا احساس دلا رہا ہو، مُبہم ہو، صحیح نہیں لگ رہا ہو یا اگر اُس میں کمزور گرائمر کا استعمال ہوا ہو، تو ہو سکتا ہے کہ یہ ایک حملہ ہو- آپ ہمیشہ مشکوک رہیں کیونکہ اکثر اپنی عقل سلیم کا استعمال ہی سب سے بہترین دفاع ہوتا ہے-

آپ کئی طریقوں سے رینسم ویئر سے بچ سکتے ہیں جیسے کہ ای میل اٹیچمنٹس کھولنے یا کسی لنک پر کلک کرنے سے پہلے انتہائی محتاط رہنا، اس بات کو یقینی بنانا کہ آپ کے پاس اپڈیٹڈ اینٹی وائرس سافٹ ویئر موجود ہے اور اس بات کی بھی تصدیق کرنا کہ آپ کی فائلز باقاعدگی سے بیک اپ ہو رہی ہیں اور وقت پڑنے پر ری-اسٹور ہو جائیں-

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:

فشنگ:	https://securingthehuman.sans.org//ouch/2015#december2015
میلویئر کیا ہے:	https://securingthehuman.sans.org/ouch/2016#march2016
انکرپشن:	https://securingthehuman.sans.org/ouch/2016#june2016
بیک اپس:	https://securingthehuman.sans.org/ouch/2015#august2015
مائیکروسافٹ کا مضمون:	https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
SANS FOR610 کورس – ریورس انجینئرنگ میلویئر:	https://sans.org/for610

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

ترجمہ: شعیب ہاشمی