نام: _____ تاریخ: _____ نمبر: _____

میل ویئر تجزیہ اور خطرے میں کمی گائیڈ

ٹروجنز، رینسم ویئر، اسپائی ویئر، روٹ کٹس، ورچوئلائزیشن سینڈ باکسز، کنٹینمنٹ

میل ویئر تجزیہ سیکھنے کا جائزہ

محفوظ شدہ
ڈیٹا کی خفیہ کاری
256 بٹ AES معیار

تعمیل شدہ
عالمی معیارات
GDPR اور CCPA فریم ورکس

زیرو ٹرسٹ
رسائی کی پالیسی
ملٹی فیکٹر تصدیق

خوش آمدید! یہ سرگرمی پیکٹ آپ کو میل ویئر کے تجزیے اور روک تھام سے متعارف کراتا ہے۔ آپ اسپائی ویئر، ٹروجنز، رینسم ویئر پے لوڈز، ریورس انجینئرنگ ٹولز، روٹ کٹ کے رویے، اور روک تھام کی حکمت عملیوں کا جائزہ لیں گے۔

ورک شیٹ کے چیک پوائنٹس

- [ ] **حصہ 1-4: سائبر سیکیورٹی اور خطرات سے بچاؤ میں مہارت حاصل کریں۔**
- [ ] **حصہ 5-7: کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔**
- [ ] **حصہ 8-9: کیس اسٹڈیز اور سائفر چیلنج حل کریں۔**
- [ ] **حصہ 10: بنیادی اور اعلیٰ FAQ صفحات کا جائزہ لیں۔**
- [ ] **حصہ 11: 10 دلچسپ حقیقی دنیا کے حقائق دریافت کریں۔**
- [ ] **اضافی: تیزی سے سوچیں چیلنج**

VPN.com سائبر سیکیورٹی گائیڈ کھولیں

URL: https://www.vpn.com/cybersecurity/malware/

آپ کی میل ویئر سے بچاؤ کا لرننگ روڈ میپ

- ٹروجن، ورم اور روٹ کٹ میل ویئر کی اقسام میں فرق واضح کریں۔
- کوڈ کے تجزیے کے لیے سینڈ باکس ورچوئلائزیشن ایگزیکیوشن نافذ کریں۔
- فعال رینسم ویئر پے لوڈز کے لیے روک تھام اور صفائی کے منصوبے ڈیزائن کریں۔

میل ویئر تجزیہ گائیڈ ہدایات

کثیر انتخابی اور درست/غلط سوالات حل کریں، لفظوں کے ذخیرے کی مدد سے خالی جگہیں پُر کریں، تعریفوں کا ملان کریں، اور کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔ اپنے علم کو میل ویئر کی روک تھام پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

میل ویئر کا تجزیہ اور خطرے پر قابو (تعارف)

ٹروجنز، ورمز اور رینسم ویئر جیسا نقصان دہ کوڈ اینڈ پوائنٹس اور سرورز کے لیے زیادہ اثر والے خطرات پیدا کرتا ہے۔ سیکیورٹی ٹیمیں میل ویئر کا تجزیہ ورچوئل سینڈ باکسز میں کرتی ہیں اور پے لوڈ کے پھیلاؤ کو روکنے کے لیے فوری نیٹ ورک تنہائی کے اقدامات کرتی ہیں۔

ہر چیک پوائنٹ کو غور سے پڑھیں اور درست جواب منتخب کریں یا لکھیں۔

چیک پوائنٹ 1: کثیر انتخابی چیلنج

1. ٹروجن ہارس کی بنیادی خصوصیت کیا ہے؟
   - A. یہ جائز سافٹ ویئر کا روپ دھارتا ہے تاکہ صارفین کو اسے چلانے پر آمادہ کرے
   - B. یہ مقامی نیٹ ورک لائنوں پر خودکار طور پر پھیل جاتا ہے
   - C. یہ الگ تھلگ ورچوئل سینڈ باکسز کے اندر فائلوں کو متاثر کرتا ہے
   - D. یہ انٹرنیٹ سروس پرووائیڈر کے ٹریفک کو روکتا ہے

2. کس قسم کا میل ویئر فائلوں کو خفیہ کرتا ہے اور ادائیگی کا مطالبہ کرتا ہے؟
   - A. رینسم ویئر
   - B. اسپائی ویئر
   - C. روٹ کٹ
   - D. ایڈ ویئر

3. اسپائی ویئر کی نمائندگی کیا کرتا ہے؟
   - A. میل ویئر جو صارف کے کی اسٹروکس اور براؤزر سرگرمیوں کی خفیہ نگرانی کے لیے بنایا گیا ہو
   - B. سینڈ باکس والے ورچوئل کنٹینر کے اندر چلنے والا پروگرام کوڈ
   - C. ڈیٹا بیس رجسٹریوں سے ڈاؤن لوڈ کی گئی اینٹی میل ویئر اپ ڈیٹس
   - D. اسکرین کی روشنی کی خودکار ایڈجسٹمنٹ

4. میل ویئر ڈیولپرز روٹ کٹس کیوں استعمال کرتے ہیں؟
   - A. فعال پروسیسز اور بدنیت فائلوں کو آپریٹنگ سسٹم سے چھپانا
   - B. اینڈ پوائنٹس پر CPU پروسیسنگ کی رفتار بڑھانے کے لیے
   - C. ڈیٹا بیس فائلوں کو محفوظ کلاؤڈ والٹس میں بیک اپ کرنے کے لیے
   - D. لیپ ٹاپس کی بیٹری کی عمر بہتر بنانے کے لیے

5. میل ویئر کے تجزیے میں سینڈ باکسنگ کا کیا مطلب ہے؟
   - A. مشتبہ فائلوں کو الگ تھلگ ورچوئل والٹ میں چلا کر رویے کا محفوظ مشاہدہ کرنا
   - B. فائل ہیشز کو معروف خطرات کے ڈیٹا بیس سے ملا کر اسکین کرنا
   - C. دراندازی کے بعد ڈیٹا بیس بیک اپس بحال کرنا
   - D. مقامی نیٹ ورک راؤٹرز کو عوامی لائنوں سے منقطع کرنا

چیک پوائنٹ 2: درست یا غلط چیلنج

6 سوال 6

6. کمپیوٹر کیڑوں کو مقامی نیٹ ورکس میں پھیلنے کے لیے انسانی صارف کی مداخلت درکار ہوتی ہے۔

درست غلط

7 سوال 7

7. ایڈ ویئر ہمیشہ بے ضرر ہوتا ہے اور صارف کے رویے یا براؤزر ہسٹری کو ٹریک نہیں کرتا۔

درست غلط

8 سوال 8

8. صاف آف لائن بیک اپس بحال کرنے سے متاثرین تاوان ادا کیے بغیر خفیہ شدہ فائلیں واپس حاصل کر سکتے ہیں۔

درست غلط

9 سوال 9

9. سگنیچر پر مبنی اینٹی وائرس زیرو ڈے میل ویئر کو اس کا سگنیچر موجود ہونے سے پہلے ہی قابل اعتماد طریقے سے روک لیتا ہے۔

درست غلط

10 سوال 10

10. فائل لیس میل ویئر نقصان دہ اسکرپٹس سسٹم میموری میں چلاتا ہے اور ڈسک پر فائلیں لکھنے سے بچتا ہے۔

درست غلط

چیک پوائنٹ 3: کلیدی اصطلاح شامل کرنا

ذیل میں ہر جملہ پڑھیں اور خالی جگہ کو ورڈ بینک سے درست اصطلاح کے ساتھ پُر کریں۔

1. محفوظ یوٹیلیٹی پروگرام کے بھیس میں چھپا میل ویئر _____ ہوتا ہے۔
2. رقم کے لیے ڈیٹابیس سسٹمز کو لاک کرنے والے نقصان دہ پے لوڈز _____ کی نمائندگی کرتے ہیں۔
3. پاس ورڈز کو خفیہ طور پر ریکارڈ کرنے والے کی لاگرز _____ کی مثال ہیں۔
4. آپریٹنگ سسٹم کرنلز میں گہرائی میں چھپنے کے لیے _____ درکار ہوتا ہے۔
5. مشتبہ فائلوں کا الگ تھلگ والٹ میں تجزیہ کرنے کے لیے ورچوئل _____ استعمال ہوتا ہے۔
6. فعال میل ویئر پے لوڈز کا پھیلاؤ روکنے کے لیے نیٹ ورک کی فوری _____ ضروری ہے۔

الفاظ کا بینک

اسپائی ویئر | ٹروجن | روٹ کٹ | روک تھام | رینسم ویئر | سینڈ باکس | فائل لیس | ورم

اپنے جوابات یہاں لکھیں:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

چیک پوائنٹ 4: سیکیورٹی تصورات کا ملان

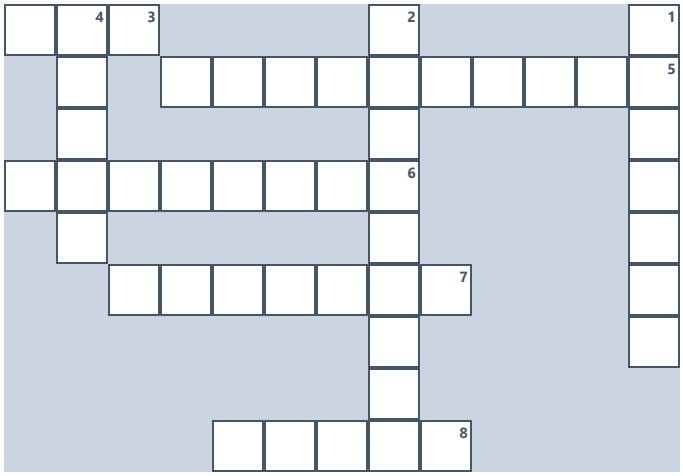
تعریفوں کا ملان

دائیں جانب کی ہر اصطلاح کو بائیں جانب کی درست تعریف سے ملائیں اور بھرے جانے والے ان پٹ باکس میں متعلقہ حرف (A-H) لکھیں۔

1. ٹروجن	A	ایسا پروگرام جو صارف کی سرگرمی اور ان پٹ کو خفیہ طور پر مانیٹر اور ریکارڈ کرنے کے لیے بنایا گیا ہو۔
2. رینسم ویئر	B	میل ویئر جو ڈسک اسکینرز کی نظر سے بچنے کے لیے براہِ راست RAM میں چلتا ہے۔
3. اسپائی ویئر	C	خطرناک پے لوڈز کے پھیلاؤ کو روکنے کے لیے متاثرہ اینڈ پوائنٹس کو محدود کرنا۔
4. روٹ کٹ	D	نقصان دہ سافٹ ویئر جو بے ضرر یا مفید یوٹیلیٹی پروگرام کا روپ دھارے۔
5. سینڈ باکس	E	خود کو دہرانے والا میل ویئر جو انسانی عمل کے بغیر نیٹ ورکس میں پھیلتا ہے۔
6. روک تھام	F	میل ویئر جو سسٹم اسٹوریج کو خفیہ کرتا ہے اور کی فراہم کرنے کے لیے ادائیگی کا مطالبہ کرتا ہے۔
7. ورم	G	بدنیت فائلوں کا محفوظ تجزیہ کرنے کے لیے استعمال ہونے والا الگ تھلگ ورچوئل ماحول۔
8. فائل لیس	H	خفیہ میل ویئر جو انتظامی کنٹرول برقرار رکھنے کے لیے سسٹم کرنلز میں گہرائی میں چھپ جاتا ہے۔

چیک پوائنٹ 5: کراس ورڈ پہیلی

فعال سفید خانوں میں حروف ٹائپ کر کے کراس ورڈ پہیلی حل کریں۔ نمبر نیچے دیے گئے سراغوں سے مطابقت رکھتے ہیں۔



افقی

3. خود کو نقل کرنے والا میل ویئر جو انسانی عمل کے بغیر نیٹ ورکس میں پھیلتا ہے (3)

5. ایسا پروگرام جو صارف کی سرگرمی اور ان پٹ کو خفیہ طور پر مانیٹر اور ریکارڈ کرنے کے لیے بنایا گیا ہو (10)

6. الگ تھلگ ورچوئل ماحول جو نقصان دہ فائلوں کا محفوظ تجزیہ کرنے کے لیے استعمال ہوتا ہے (8)

7. متاثرہ اینڈ پوائنٹس کو محدود کرنا تاکہ خطرناک پے لوڈز کا پھیلاؤ رکے (7)

8. ایسا نقصان دہ سافٹ ویئر جو بے ضرر یا مفید یوٹیلیٹی پروگرام کے بھیس میں ہوتا ہے (5)

عمودی

1. وہ میل ویئر جو ڈسک اسکینرز سے بچنے کے لیے براہ راست RAM میں چلتا ہے (7)

2. وہ میل ویئر جو سسٹم اسٹوریج کو انکرپٹ کر کے کلید دینے کے لیے ادائیگی مانگتا ہے (9)

4. سسٹم کرنلز میں گہرائی میں چھپا ہوا میل ویئر جو انتظامی کنٹرول برقرار رکھتا ہے (5)

چیک پوائنٹ 5 – متبادل سرگرمی: قابلِ رسائی کراس ورڈ سراغ

اسکرین ریڈر اور کی بورڈ استعمال کرنے والے صارفین نیچے دیے گئے ٹیکسٹ فیلڈز میں کراس ورڈ کے جوابات براہ راست ٹائپ کر سکتے ہیں۔

افقی

3 افقی: خود کو نقل کرنے والا میل ویئر جو انسانی عمل کے بغیر نیٹ ورکس میں پھیلتا ہے (3 حروف):

5 افقی: ایسا پروگرام جو صارف کی سرگرمی اور ان پٹ کو خفیہ طور پر مانیٹر اور ریکارڈ کرنے کے لیے بنایا گیا ہو (10 حروف):

6 افقی: الگ تھلگ ورچوئل ماحول جو نقصان دہ فائلوں کا محفوظ تجزیہ کرنے کے لیے استعمال ہوتا ہے (8 حروف):

7 افقی: متاثرہ اینڈ پوائنٹس کو محدود کرنا تاکہ خطرناک پے لوڈز کا پھیلاؤ رکے (7 حروف):

8 افقی: ایسا نقصان دہ سافٹ ویئر جو بے ضرر یا مفید یوٹیلیٹی پروگرام کے بھیس میں ہوتا ہے (5 حروف):

عمودی

1 عمودی: وہ میل ویئر جو ڈسک اسکینرز سے بچنے کے لیے براہ راست RAM میں چلتا ہے (7 حروف):

2 عمودی: وہ میل ویئر جو سسٹم اسٹوریج کو انکرپٹ کر کے کلید دینے کے لیے ادائیگی مانگتا ہے (9 حروف):

4 عمودی: سسٹم کرنلز میں گہرائی میں چھپا ہوا میل ویئر جو انتظامی کنٹرول برقرار رکھتا ہے (5 حروف):

چیک پوائنٹ 6: پوشیدہ الفاظ کی تلاش

نیچے گرڈ میں چھپی 8 اہم اصطلاحات تلاش کریں۔ الفاظ افقی، عمودی یا ترچھے ہو سکتے ہیں۔

پ	و	د	ج	گ	ن	ک	ف	م	ڈ	ن	ل	پ	ی	ہ
ہ	ٹ	ٹ	ش	ر	ب	ا	ا	ب	پ	ٹ	ل	ھ	ش	س
ھ	ش	ک	ڈ	ی	س	ت	ئ	ن	ک	ر	ر	ت	د	گ
ر	گ	ٹ	س	ن	م	چ	ل	ک	ک	و	ن	و	ہ	ی
ئ	ی	و	چ	پ	ا	ہ	ل	م	ل	چ	د	و	س	ب
ی	ئ	ر	ت	ہ	س	ف	ی	ے	پ	ن	ف	ئ	ی	چ
و	س	چ	ف	ت	پ	گ	س	ر	ت	ن	ڈ	م	ن	پ
م	ی	ب	ا	ف	گ	ت	و	ش	ا	ت	ت	ل	ڈ	ت
س	ٹ	چ	د	ت	ئ	و	ن	ک	ک	ٹ	د	و	ب	ف
ن	ہ	ٹ	ن	ے	ی	و	ٹ	ت	ا	ا	ن	ل	ا	گ
ی	م	ی	ڈ	ن	و	ر	س	ھ	و	ی	و	پ	ک	گ
ر	ھ	ب	ج	و	ی	م	ڈ	ا	ئ	ر	ا	و	س	ف
ھ	ھ	ش	ج	د	ئ	ک	ن	م	س	ک	ک	ہ	ل	چ
م	ن	چ	ف	ا	ر	ل	ے	ج	ے	ب	ھ	و	ھ	ب
چ	ک	ف	ج	س	ل	م	گ	ڈ	پ	ک	ف	ھ	چ	ھ

الفاظ کی فہرست

ٹروجن
رینسمویئر
اسپائیویئر
روٹکٹ
سینڈباکس
روکتھام
ورم
فائللیس

چیک پوائنٹ 6 – متبادل سرگرمی: قابلِ رسائی الفاظ کا ملان

ورڈ سرچ کی 8 اصطلاحات میں سے ہر ایک کو اس کی درست تعریف سے ملائیں اور خالی جگہ میں حرف (A-H) لکھیں۔

اصطلاحات
A. ٹروجن
B. رینسمویئر
C. اسپائیویئر
D. روٹکٹ
E. سینڈباکس
F. روکتھام
G. ورم
H. فائللیس

	تعریفیں اور ملان کے خانے
	1. سسٹم کرنلز میں گہرائی میں چھپا ہوا میل ویئر جو انتظامی کنٹرول برقرار رکھتا ہے۔
	2. متاثرہ اینڈ پوائنٹس کو محدود کرنا تاکہ خطرناک پے لوڈز کا پھیلاؤ رکے۔
	3. وہ میل ویئر جو ڈسک اسکینرز سے بچنے کے لیے براہ راست RAM میں چلتا ہے۔
	4. خود کو نقل کرنے والا میل ویئر جو انسانی عمل کے بغیر نیٹ ورکس میں پھیلتا ہے۔
	5. وہ میل ویئر جو سسٹم اسٹوریج کو انکرپٹ کر کے کلید دینے کے لیے ادائیگی مانگتا ہے۔
	6. ایسا پروگرام جو صارف کی سرگرمی اور ان پٹ کو خفیہ طور پر مانیٹر اور ریکارڈ کرنے کے لیے بنایا گیا ہو۔
	7. ایسا نقصان دہ سافٹ ویئر جو بے ضرر یا مفید یوٹیلیٹی پروگرام کے بھیس میں ہوتا ہے۔
	8. الگ تھلگ ورچوئل ماحول جو نقصان دہ فائلوں کا محفوظ تجزیہ کرنے کے لیے استعمال ہوتا ہے۔

چیک پوائنٹ 7: الجھے الفاظ کا چیلنج

سائبر سیکیورٹی کے اہم تصورات اور اصطلاحات ظاہر کرنے کے لیے نیچے دیے گئے حروف کو درست ترتیب میں لائیں۔ اپنے جوابات دیے گئے ان پٹ باکسز میں لکھیں۔

1. ج و ٹ ن ر
2. ئ ا ا س ئ ر و ی ی پ
3. ڈ ی س ب ا س ک ن
4. ر م و
5. ی م ی ر و س ر ئ ن
6. ک ر ٹ ٹ و
7. ر ا ھ م و ت ک
8. ا ل س ف ی ل ئ

اضافی سرگرمی: تیزی سے سوچیں

ہر زمرے کے لیے 3 جوابات لکھیں۔ جو سب سے پہلے فہرست مکمل کرے وہ جیتتا ہے۔

1	محفوظ ایپس ڈاؤن لوڈ کرنے کے مقامات		
2	وہ ڈیوائسز جنہیں ہیک کیا جا سکتا ہے		
3	وہ چیزیں جن کا آپ بیک اپ لیتے ہیں		
4	ای میل میں انتباہی علامات		
5	فون میں میل ویئر کی علامات		
6	آپ کی جانی پہچانی میل ویئر کی اقسام		
7	وہ فائل اقسام جن سے احتیاط ضروری ہے		
8	PC پر میل ویئر آنے کے طریقے		
9	محفوظ عادات جو آپ آج شروع کر سکتے ہیں		
10	سائبر سیکیورٹی سے متعلق الفاظ		
11	ڈیٹا لیک کے بعد کرنے کے کام		
12	سافٹ ویئر اپ ڈیٹ کرنے کی وجوہات		
13	میل ویئر سے ملتے جلتے ناموں والے جانوروں یا کرداروں کے نام		
14	وہ چیزیں جو میل ویئر چرا سکتا ہے		
15	غلط لنک پر کلک کرنے کی صورت میں کرنے کے کام		

چیک پوائنٹ 8: سائبر سیکیورٹی کیس اسٹڈیز

جو تصورات آپ نے سیکھے ہیں انہیں نیچے دیے گئے حقیقی منظرناموں کو حل کرنے میں استعمال کریں۔

کیس اسٹڈی 1: انٹرپرائز رینسم ویئر پے لوڈ کی روک تھام



منظرنامہ: ایک کارپوریٹ لوکل ایریا نیٹ ورک فعال رینسم ویئر کی زد میں آ گیا ہے۔ اہم فائل سرورز پر .locked کے ساتھ فائل ایکسٹینشنز نظر آنے لگی ہیں۔ محدود کرنے کی پالیسیاں قائم کریں۔

بحث کا سوال: کنٹینمنٹ کے اقدامات تفصیل سے بیان کریں، اور ڈیٹا ریکوری کا پروٹوکول بیان کریں۔

کیس اسٹڈی 2: فائل لیس میل ویئر کی میموری انجیکشن



منظرنامہ: ایک تجزیہ کار معیاری انتظامی ٹولز استعمال کرتے ہوئے غیر مستقل سسٹم RAM میں براہ راست چلنے والے مشکوک اسکرپٹنگ پیٹرنز کا پتا لگاتا ہے، لیکن ڈسک پر کوئی نقصان دہ فائل موجود نہیں ہے۔

بحث کا سوال: میموری اینالیسس کی حکمت عملی واضح کریں، اور فائل لیس ایگزیکیوشن کو بلاک کرنے والے ٹولز بیان کریں۔

چیک پوائنٹ 9: سائفر حل کریں

سائبر سیکیورٹی پیشہ ور نیٹ ورک اثاثوں کو آن لائن خطرات پیدا کرنے والوں سے بچاتا ہے۔ نیچے دی گئی حرف سے عدد کی کلید استعمال کر کے خالی جگہوں میں متعلقہ حروف لکھ کر پیغام ڈی کرپٹ کریں۔

حرف سے عدد خفیہ کاری کی کلید

ا=1 ب=2 پ=3 ت=4 ٹ=5 ث=6 ج=7 چ=8 ح=9 خ=10 د=11 ڈ=12 ذ=13

ر=14 ڑ=15 ز=16 ژ=17 س=18 ش=19 ص=20 ض=21 ط=22 ظ=23 ع=24 غ=25 ف=26

ق=27 ک=28 گ=29 ل=30 م=31 ن=32 ں=33 و=34 ہ=35 ھ=36 ی=37 ے=38 ئ=39

16	12	34	30		38	3		38	18		16	14	5	37	32	1	31

33	37	32	1	8	35	3

ڈی کوڈ شدہ پیغام:

ٹپ: ہر نمبر اوپر دی گئی کلید کے ایک اردو حرف کو ظاہر کرتا ہے۔

چیک پوائنٹ 10: سائبر سیکیورٹی عمومی سوالات – بنیادی (حصہ A)

آن لائن خطرات کی روک تھام کے بارے میں عام سوالات اور جوابات کا جائزہ لیں۔

Q1: میلویئر کیا ہے؟

نقصان دہ سافٹ ویئر جو خطرہ پیدا کرنے والے عناصر آلات اور نیٹ ورکس کو نقصان پہنچانے، ہائی جیک کرنے یا ڈیٹا چرانے کے لیے بناتے ہیں۔

Q2: وائرس اور ورم میں کیا فرق ہے؟

وائرس کو پھیلنے کے لیے انسانی عمل (جیسے فائل کھولنا) درکار ہوتا ہے، جبکہ ورم نیٹ ورکس میں خودکار طور پر پھیلتا ہے۔

Q3: ٹروجن ہارس کمپیوٹر کو کیسے متاثر کرتا ہے؟

یہ صارفین کو بے ضرر یا محفوظ پروگرام کا روپ دھار کر دھوکا دیتا ہے اور اپنا بدنیت پے لوڈ اندر چھپائے رکھتا ہے۔

Q4: رینسم ویئر کیا ہے؟

میل ویئر کی قسم جو ہدف سسٹم پر فائلیں خفیہ کر دیتی ہے اور ڈی کرپشن کلید کے بدلے مالی ادائیگی طلب کرتی ہے۔ [1]

Q5: اسپائی ویئر کیا ہے؟

نقصان دہ سافٹ ویئر جو خفیہ طور پر صارف کی کی اسٹروکس، پاس ورڈز اور براؤزنگ عادات ریکارڈ کر کے حملہ آوروں کو بھیجتا ہے۔

چیک پوائنٹ 10: سائبر سیکیورٹی عمومی سوالات – بنیادی (حصہ B)

آن لائن خطرات کی روک تھام کے بارے میں عام سوالات اور جوابات کا جائزہ لیں۔

Q6: سینڈ باکسنگ کا کیا مطلب ہے؟

پروڈکشن سسٹمز کو خطرے میں ڈالے بغیر مشکوک فائلوں کے رویے کا مشاہدہ کرنے کے لیے انہیں محفوظ، الگ تھلگ ورچوئل ماحول میں چلانا۔

Q7: فائل لیس میل ویئر کیا ہے؟

میل ویئر جو جائز یوٹیلیٹیز استعمال کرتے ہوئے براہِ راست سسٹم میموری (RAM) میں چلتا ہے اور بنیادی اسکینرز سے بچنے کے لیے ڈسک پر فائلیں نہیں لکھتا۔

Q8: روٹ کٹ میل ویئر کا تحفظ کیسے کرتا ہے؟

یہ بدنیت پروسیسز اور فائلوں کو چھپاتا ہے، اکثر آپریٹنگ سسٹم کرنل کو تبدیل کر کے، اس لیے اینٹی وائرس اسکینرز انہیں نظر انداز کر سکتے ہیں۔

Q9: متحرک رویے کی نگرانی کیا ہے؟

ایسی اینٹی وائرس اسکیننگ جو فعال پروسیسز کی حقیقی وقت میں نگرانی کر کے میل ویئر کی مخصوص کارروائیوں، جیسے بڑی تعداد میں فائلوں کی خفیہ کاری، کو بلاک کرتی ہے۔

Q10: انسیڈنٹ رسپانس کے دوران روک تھام فوری کیوں ہے؟

متاثرہ اینڈ پوائنٹس کو الگ کرنے سے فعال میل ویئر پے لوڈز دیگر نیٹ ورک ڈیوائسز تک پھیلنے سے رک جاتے ہیں۔

چیک پوائنٹ 10: سیکیورٹی عمومی سوالات – اعلیٰ (حصہ C)

سیکیورٹی فریم ورکس، میل ویئر تجزیے اور ڈیٹا کمپلائنس کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q1: میلویئر ڈیویلپرز سگنیچر پر مبنی اینٹی وائرس اسکینرز سے کیسے بچتے ہیں؟

وہ پولی مورفزم استعمال کرتے ہیں، یعنی ہر انفیکشن کے ساتھ فائل کا ہیش اور کوڈ ڈھانچہ بدل دیتے ہیں جبکہ نقصان دہ رویہ وہی رہتا ہے۔

Q2: میلویئر مہمات میں دوہرے استعمال کے ٹولز کا کیا خطرہ ہے؟

حملہ آور جائز انتظامی ٹولز (جیسے PowerShell یا Sysinternals) استعمال کر کے عام نیٹ ورک ٹریفک میں گھل مل جاتے ہیں، جس سے شناخت مشکل ہو جاتی ہے۔

Q3: پروسیس ہولوئنگ نقصان دہ پے لوڈز کو کیسے چلاتی ہے؟

یہ ایک جائز سسٹم پروسیس کو معطل حالت میں شروع کرتا ہے، اس کے میموری کوڈ کو میل ویئر سے بدل دیتا ہے، اور عمل درآمد دوبارہ شروع کر دیتا ہے۔

Q4: کمانڈ اینڈ کنٹرول (C2) سرور کا کیا کردار ہے؟

ہیکرز کا چلایا جانے والا ریموٹ سرور جو متاثرہ مشینوں پر چلنے والے میل ویئر کو ہدایات اور پے لوڈز بھیجتا ہے۔

Q5: کی لاگنگ کا پتا لگانا مشکل کیوں ہے؟

بنیادی کی اسٹروک لاگرز کم سے کم CPU وسائل استعمال کرتے ہیں اور اپنے پروسیسز کو جائز یوزر اسپیس یوٹیلیٹیز کے اندر چھپا لیتے ہیں۔

چیک پوائنٹ 10: سیکیورٹی عمومی سوالات – اعلیٰ (حصہ D)

سیکیورٹی فریم ورکس، میل ویئر تجزیے اور ڈیٹا کمپلائنس کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q6: کوڈ اوبفسکیشن میل ویئر کے تجزیے میں تاخیر کیسے کرتی ہے؟

یہ سورس کوڈ کو خفیہ یا دوبارہ ترتیب دیتا ہے، جس سے وہ تجزیہ کاروں کے ٹولز اور سیکیورٹی اسکینرز کے لیے ناقابل مطالعہ ہو جاتا ہے۔

Q7: بوٹ کٹ کا کیا کام ہے؟

روٹ کٹ جو بوٹ پروسیس (MBR، بوٹ سیکٹر یا UEFI فرم ویئر) کو متاثر کرتی ہے، اس لیے یہ آپریٹنگ سسٹم لوڈ ہونے سے پہلے چلتی ہے۔

Q8: ہیورسٹک اسکیننگ زیرو ڈے خطرات کی شناخت کیسے کرتی ہے؟

یہ ڈیٹا بیس ہیش کے ملان کو دیکھنے کے بجائے مشتبہ کوڈ پیٹرنز اور انتظامی کمانڈز کو اسکین کرتا ہے۔

Q9: DLL ہائی جیکنگ کا کیا خطرہ ہے؟

کسی جائز ایپلی کیشن کو اس کی ڈائریکٹری پاتھ میں رکھ کر ایک بدنیت ڈائنامک لنک لائبریری (DLL) لوڈ کرنے پر مجبور کرنا۔

Q10: خودکار میلویئر تجزیاتی پائپ لائنز ورچوئلائزیشن کیسے استعمال کرتی ہیں؟

وہ مشکوک فائلوں کو متعدد OS VMs میں چلاتے ہیں اور خود بخود رویے کے لاگز اور نیٹ ورک PCAP فائلیں بناتے ہیں۔

حصہ 11: 10 حقیقی دنیا کے سائبر سیکیورٹی حقائق اور بصیرتیں

سیکیورٹی خلاف ورزیوں، دفاعی نظاموں اور تعمیل کے معیارات کے بارے میں حقیقی دنیا کے حقائق کا جائزہ لیں۔

1. سیکیورٹی بصیرت

ٹروجن ہارس انفیکشن کا ایک عام طریقہ بنے ہوئے ہیں کیونکہ وہ نقصان دہ کوڈ کو بظاہر بے ضرر پروگراموں کے اندر چھپاتے ہیں۔

2. سیکیورٹی بصیرت

FBI کے IC3 کو 2025 میں رینسم ویئر کی 3,600 سے زیادہ شکایات موصول ہوئیں، جن میں رپورٹ شدہ نقصانات 32 ملین ڈالر سے زیادہ تھے۔ [3]

3. سیکیورٹی بصیرت

کیڑے (ورمز) بغیر پیچ شدہ پروٹوکول کمزوریوں، جیسے SMB میں EternalBlue، کا فائدہ اٹھا کر نیٹ ورکس میں تیزی سے پھیل سکتے ہیں۔

4. سیکیورٹی بصیرت

فائل لیس میل ویئر کا پتا لگانا مشکل ہے کیونکہ یہ جائز ٹولز کے ذریعے میموری میں چلتا ہے اور ڈسک پر بہت کم نشانات چھوڑتا ہے۔

5. سیکیورٹی بصیرت

تجزیاتی سینڈ باکسز عموماً ہر رن کے بعد صاف اسنیپ شاٹ پر واپس چلے جاتے ہیں تاکہ ہر ٹیسٹ معلوم حالت سے شروع ہو۔

6. سیکیورٹی بصیرت

روٹ کٹس کرنل سسٹم کالز میں ترمیم کر سکتے ہیں اور اینٹی میل ویئر اسکینرز کو جعلی تشخیصی نتائج بتا سکتے ہیں۔

7. سیکیورٹی کی بصیرت

کوڈ اوبفسکیشن پیکر یوٹیلیٹیز استعمال کر کے میل ویئر کے اصل بائنری پے لوڈ کی ساخت کو دبا کر چھپاتی ہے۔

8. سیکیورٹی کی بصیرت

پولی مارفک میلویئر ہر نئی کاپی کے ساتھ اپنا کوڈ، اور اس طرح اپنی فائل ہیش، بدل لیتا ہے تاکہ سگنیچر چیکس سے بچ سکے۔

9. سیکیورٹی کی بصیرت

DLL ہائی جیکنگ Windows جیسے معیاری آپریٹنگ سسٹمز میں سرچ آرڈر کی کنفیگریشنز کا فائدہ اٹھاتی ہے۔

10. سیکیورٹی بصیرت

سیکیورٹی وینڈرز روزانہ میل ویئر کے بہت بڑی تعداد میں نئے نمونے دریافت کرتے ہیں، اس لیے سگنیچرز کو مسلسل اپ ڈیٹ کی ضرورت ہوتی ہے۔

تکنیکی حوالہ جات اور ماخذ

مطالعاتی گائیڈ اور انٹرایکٹو پہیلیاں عالمی NIST، OWASP اور ڈیٹا پرائیویسی کمپلائنس معیارات سے مرتب کی گئی ہیں۔

علمی اور صنعتی حوالہ جات

[1] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

جوابی کلید: چیک پوائنٹ 1 – کثیر انتخابی

1 سوال 1 — درست جواب: A

تدریسی نوٹ

ٹروجن ہارس کی بنیادی خصوصیت کیا ہے؟ → یہ جائز سافٹ ویئر کا روپ دھارتا ہے تاکہ صارفین کو اسے چلانے پر آمادہ کرے

2 سوال 2 — درست جواب: A

تدریسی نوٹ

کس قسم کا میل ویئر فائلوں کو خفیہ کرتا ہے اور ادائیگی کا مطالبہ کرتا ہے؟ → رینسم ویئر

3 سوال 3 — درست جواب: A

تدریسی نوٹ

اسپائی ویئر کی نمائندگی کیا کرتا ہے؟ → میل ویئر جو صارف کے کی اسٹروکس اور براؤزر سرگرمیوں کی خفیہ نگرانی کے لیے بنایا گیا ہو

4 سوال 4 — درست جواب: A

تدریسی نوٹ

میل ویئر ڈیولپرز روٹ کٹس کیوں استعمال کرتے ہیں؟ → فعال پروسیسز اور بدنیت فائلوں کو آپریٹنگ سسٹم سے چھپانا

5 سوال 5 — درست جواب: A

تدریسی نوٹ

میل ویئر کے تجزیے میں سینڈ باکسنگ کا کیا مطلب ہے؟ → مشتبہ فائلوں کو الگ تھلگ ورچوئل والٹ میں چلا کر رویے کا محفوظ مشاہدہ کرنا

جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

6 سوال 6

درست جواب: غلط

تدریسی نوٹ

غلط: ورمز خود کو نقل کرتے ہیں اور صارف کے کسی عمل کے بغیر نیٹ ورکس میں پھیل جاتے ہیں۔

7 سوال 7

درست جواب: غلط

تدریسی نوٹ

غلط: ایڈ ویئر ہمیشہ بے ضرر نہیں ہوتا؛ اس میں سے بہت سا اشتہارات کو ہدف بنانے کے لیے براؤزنگ کو ٹریک کرتا ہے۔

8 سوال 8

درست جواب: درست

تدریسی نوٹ

درست: صاف آف لائن بیک اپس ادائیگی کے بغیر خفیہ شدہ فائلیں بحال کرتے ہیں، اگرچہ چرایا گیا ڈیٹا پھر بھی لیک ہو سکتا ہے۔

9 سوال 9

درست جواب: غلط

تدریسی نوٹ

غلط: سگنیچر اسکینرز کو معلوم نمونہ درکار ہوتا ہے، اس لیے بالکل نیا زیرو ڈے میل ویئر ان سے بچ کر نکل سکتا ہے۔

10 سوال 10

درست جواب: درست

تدریسی نوٹ

فائل لیس میل ویئر نقصان دہ اسکرپٹس سسٹم میموری میں چلاتا ہے اور ڈسک پر فائلیں لکھنے سے بچتا ہے۔

الفاظ کی کلید اور درجہ بندی کا معیار

استاد کی گریڈنگ روبرک: ہر درست ملان (کل 8 نمبر) اور سیاقی اصطلاح (کل 6 نمبر) کے لیے 1 نمبر دیں۔

چیک پوائنٹ 4: جوابی کلید – تصورات کا ملان

D 1. ٹروجن	F 2. رینسم ویئر	A 3. اسپائی ویئر	H 4. روٹ کٹ
G 5. سینڈ باکس	C 6. روک تھام	E 7. ورم	B 8. فائل لیس

چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

1 ٹروجن	2 رینسم ویئر	3 اسپائی ویئر	4 روٹ کٹ
5 سینڈ باکس	6 روک تھام		

چیک پوائنٹ 6 – متبادل سرگرمی: جوابی کلید – الفاظ کا ملان

1 D – روٹکٹ	2 F – روکتھام	3 H – فائللیس	4 G – ورم
5 B – رینسمویئر	6 C – اسپائیویئر	7 A – ٹروجن	8 E – سینڈباکس

اساتذہ کے لیے بحث کے نوٹس

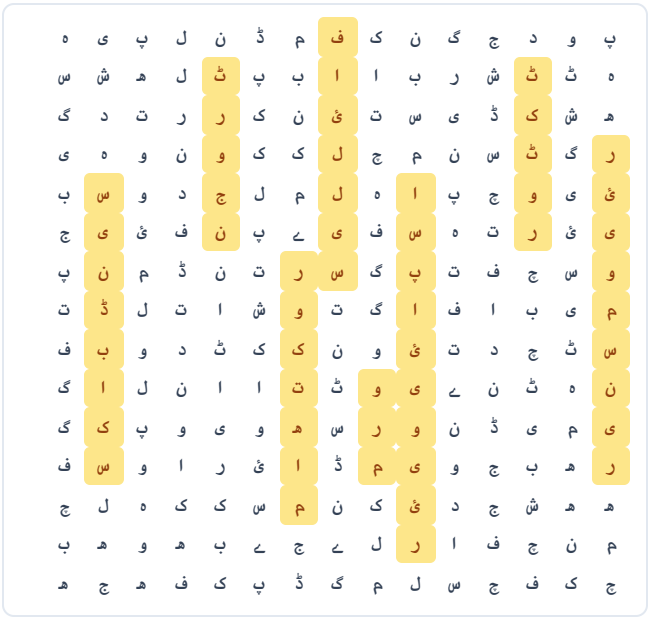
اہم اصطلاحات:
یقینی بنائیں کہ طلبہ ٹروجن، رینسم ویئر اور اسپائی ویئر کو اپنے الفاظ میں سمجھا سکیں اور ہر ایک کی مثال دے سکیں۔

کیس اسٹڈیز:
طلبہ سے کہیں کہ اپنی سفارشات کو ورک شیٹ کے حقائق پر مبنی رکھیں، ذاتی رائے پر نہیں۔

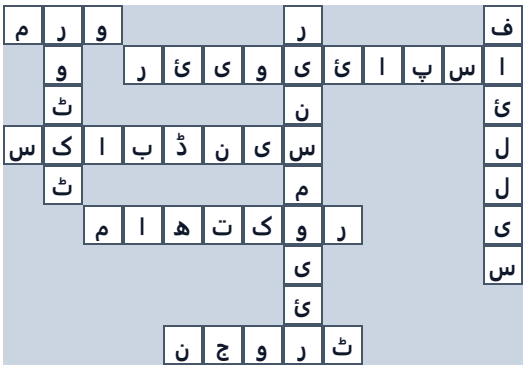
ماخذ کی جانچ:
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

پہیلیوں کی کلیدیں اور استاد کے نوٹس

الفاظ کی تلاش کا حل



کراس ورڈ کا حل



کراس ورڈ حل کے لیے استاد کی گائیڈ

افقی

3 افقی: ورم خود کو نقل کرنے والا میل ویئر جو انسانی عمل کے بغیر نیٹ ورکس میں پھیلتا ہے (3 حروف)

5 افقی: اسپائیویئر ایسا پروگرام جو صارف کی سرگرمی اور ان پٹ کو خفیہ طور پر مانیٹر اور ریکارڈ کرنے کے لیے بنایا گیا ہو (10 حروف)

6 افقی: سینڈباکس الگ تھلگ ورچوئل ماحول جو نقصان دہ فائلوں کا محفوظ تجزیہ کرنے کے لیے استعمال ہوتا ہے (8 حروف)

7 افقی: روکتھام متاثرہ اینڈ پوائنٹس کو محدود کرنا تاکہ خطرناک پے لوڈز کا پھیلاؤ رکے (7 حروف)

8 افقی: ٹروجن ایسا نقصان دہ سافٹ ویئر جو بے ضرر یا مفید یوٹیلیٹی پروگرام کے بھیس میں ہوتا ہے (5 حروف)

عمودی

1 عمودی: فائللیس وہ میل ویئر جو ڈسک اسکینرز سے بچنے کے لیے براہ راست RAM میں چلتا ہے (7 حروف)

2 عمودی: رینسمویئر وہ میل ویئر جو سسٹم اسٹوریج کو انکرپٹ کر کے کلید دینے کے لیے ادائیگی مانگتا ہے (9 حروف)

4 عمودی: روٹکٹ سسٹم کرنلز میں گہرائی میں چھپا ہوا میل ویئر جو انتظامی کنٹرول برقرار رکھتا ہے (5 حروف)

الفاظ کی ترتیب اور سائفر حل کی کلید

الفاظ کی ترتیب درست کرنے کی سرگرمی اور Secret Cipher Challenge کی گریڈنگ کلید۔

الفاظ کی ترتیب درست کرنے کی کلید

1. جوٹنر
2. ئااسئرووپپ
3. ڈیسباسکن
4. رمو
5. یمیروسرئن
6. کرٹٹو
7. راھموتک
8. السفیلئ

ٹروجن
اسپائیویئر
سینڈباکس
ورم
رینسمویئر
روٹکٹ
روکتھام
فائلللیس

خفیہ سائفر چیلنج کی کلید

"مانیٹرز سے پے لوڈز پہچانیں"

کیس اسٹڈیز کی جوابی کلید

A کیس اسٹڈی 1: انٹرپرائز رینسم ویئر پے لوڈ کی روک تھام

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک کارپوریٹ لوکل ایریا نیٹ ورک میں فعال رینسم ویئر داخل ہو گیا ہے۔ اہم فائل سرورز پر فائل ایکسٹینشنز .locked کے ساتھ دکھائی دینے لگی ہیں۔ روک تھام کی پالیسیاں قائم کریں۔
- تجویز کردہ حکمت عملی اور حل: تمام متاثرہ سرورز کو لوکل ایریا نیٹ ورک سے منقطع کریں۔ فعال انتظامی سیشنز ختم کریں۔ غیر متاثرہ فائلیں محفوظ، رائٹ لاکڈ آف لائن بیک اپ سسٹم سے بحال کریں۔

B کیس اسٹڈی 2: فائل لیس میل ویئر کی میموری انجیکشن

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک تجزیہ کار معیاری انتظامی ٹولز کے ذریعے عارضی سسٹم RAM میں براہِ راست چلنے والے مشکوک اسکرپٹنگ پیٹرنز کا پتا لگاتا ہے، لیکن ڈسک پر کوئی نقصان دہ فائل موجود نہیں۔
- تجویز کردہ حکمت عملی اور حل: متاثرہ اینڈ پوائنٹس کو الگ کریں اور پہلے میموری امیج حاصل کریں۔ PowerShell اور WMI لاگز کا جائزہ لیں، AppLocker سے غیر منظور شدہ اسکرپٹس بلاک کریں، پھر پے لوڈ صاف کرنے کے لیے ری بوٹ کریں۔