نام: _____ تاریخ: _____ نمره: _____

حملات باج‌افزار و کسب‌وکار بازیابی

اجرای بار مخرب، رمزگذاری رمزنگاری‌شدهٔ فایل‌ها، پشتیبان‌های آفلاین، رویه‌های مهار و بازیابی از فاجعه.

مروری بر یادگیری حملات باج‌افزار

ایمن‌شده
رمزگذاری داده
استاندارد AES 256 بیتی

منطبق
استانداردهای جهانی
چارچوب‌های GDPR و CCPA

اعتماد صفر
سیاست دسترسی
احراز هویت چندعاملی

خوش آمدید! این بستهٔ فعالیت شما را در بررسی حملات باج‌افزار و بازیابی کسب‌وکار راهنمایی می‌کند. با اجرای بار مخرب، رمزگذاری فایل، پشتیبان‌های آفلاین، مهار تهدید، پرداخت‌های ارز دیجیتال و برنامه‌های بازیابی پس از فاجعه آشنا می‌شوید.

ایستگاه‌های بررسی کاربرگ

- ☐ **بخش 1-4: بر امنیت سایبری و پیشگیری از تهدید مسلط شوید.**
- ☐ **بخش 5-7: جدول‌های متقاطع و جدول‌های جست‌وجوی کلمه را حل کنید.**
- ☐ **بخش 8-9: مطالعات موردی و چالش رمز را حل کنید.**
- ☐ **بخش 10: صفحه‌های پرسش‌های متداول مقدماتی و پیشرفته را مرور کنید.**
- ☐ **بخش 11: 10 واقعیت جالب دنیای واقعی را کاوش کنید.**
- ☐ **تکمیلی: چالش سریع فکر کن**

باز کردن راهنمای امنیت سایبری VPN.com

URL: https://www.vpn.com/cybersecurity/ransomware-attack/

نقشهٔ راه یادگیری بازیابی از باج‌افزار شما

- میان محموله‌های تروجان، باج‌افزار و جاسوس‌افزار تمایز قائل شوید.
- فایل‌های مخرب را در محیط‌های sandbox امن تحلیل کنید.
- تدوین رویه‌های سریع جداسازی و مهار شبکه.

دستورالعمل‌های راهنمای حملات باج‌افزار

به پرسش‌های چندگزینه‌ای و درست/نادرست پاسخ دهید، جمله‌های جای‌خالی را با استفاده از بانک واژه‌ها کامل کنید، تعاریف را تطبیق دهید و جدول‌های کلمات متقاطع و جست‌وجوی کلمه را حل کنید. دانسته‌های خود را درباره بازیابی پس از باج‌افزار به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

حملات باج‌افزار و بازیابی پس از فاجعه (مقدمه)

بارهای باج‌افزار فضای ذخیره‌سازی سیستم را به‌صورت رمزنگاری‌شده قفل می‌کنند و برای کلیدهای رمزگشایی پرداخت رمزارزی می‌خواهند. کاهش این تهدید شامل قوانین انزوای شبکه، تحلیل بدافزار در سندباکس و پشتیبان‌های سرد جداشده از شبکه (air-gapped) مستحکم است.

هر ایستگاه بررسی را با دقت بخوانید و پاسخ درست را انتخاب کنید یا بنویسید.

ایستگاه بررسی 1: چالش چندگزینه‌ای

1 1. سازوکار اصلی حملهٔ باج‌افزار چیست؟

- A. رمزگذاری فایل‌های کاربر برای سلب دسترسی به سیستم
- B. تزریق دستورهای SQL مخرب به فیلدهای فرم
- C. شنود بسته‌های شبکه در اتصال Wi-Fi عمومی
- D. جعل سرایندهای ایمیل برای دور زدن اعتبارسنجی SPF

2 2. پشتیبان آفلاین (سرد) چیست؟

- A. نسخهٔ ذخیره‌ای که از شبکه جدا شده تا از انتشار بدافزار محافظت شود
- B. نسخهٔ پشتیبانی که روی هارد دیسک سرور وب اصلی ذخیره می‌شود
- C. حافظهٔ نهان موقت لاگ‌های رجیستری سیستم
- D. ابزار مدیریتی برای بازنشانی گذرواژه‌های کاربران

3 3. تیم‌های امنیتی هنگام حملهٔ باج‌افزار چگونه باید سامانه‌های آلوده را جدا کنند؟

- A. فوراً کابل‌های شبکه را جدا کنید و رابط‌های بی‌سیم را غیرفعال کنید
- B. به‌روزرسانی پایگاه داده امضاهای آنتی‌ویروس
- C. خاموش کردن سرور DNS اصلی
- D. تغییر نام پسوند فایل‌های به‌خطرافتاده

4 4. چرا نهادهای امنیتی توصیه می‌کنند خواسته‌های باج‌افزار پرداخت نشود؟

- A. پرداخت وجه مهاجمان را تشویق می‌کند و تحویل کلید رمزگشایی را تضمین نمی‌کند
- B. همهٔ بیمه‌نامه‌های سازمانی را به‌طور خودکار باطل می‌کند
- C. به‌طور خودکار همهٔ مشتریان را از طریق ایمیل مطلع می‌کند
- D. فایل‌های پشتیبان باقی‌ماندهٔ سیستم را خراب می‌کند

5 5. برنامهٔ بازیابی پس از فاجعه (DRP) چیست؟

- A. فرایندی ساختاریافته برای بازگرداندن عملیات و داده‌ها پس از نفوذ به سیستم
- B. پیکربندی دیوار آتش که پورت‌های شبکهٔ ورودی را نگاشت می‌کند
- C. طرحوارهٔ پایگاه داده که امتیازهای مدیریتی کاربران را فهرست می‌کند
- D. یک پروتکل احراز هویت ایمیل که دامنه‌های جعلی را رد می‌کند

ایستگاه بررسی 2: چالش درست یا نادرست

6 پرسش 6

6. بارهای باج‌افزار به‌راحتی می‌توانند به پشتیبان‌های آنلاین متصل به شبکه منتشر شوند.

درست نادرست

7 پرسش 7

7. پرداخت باج رمزارزی تضمین می‌کند که فایل‌ها با موفقیت رمزگشایی شوند.

درست نادرست

8 پرسش 8

8. قطع سیستم‌های آلوده از شبکه به توقف انتشار باج‌افزار به سیستم‌های مجاور کمک می‌کند.

درست نادرست

9 پرسش 9

9. باج‌افزار هرگز از رمزنگاری متقارن برای رمزگذاری فضای ذخیره‌سازی سیستم استفاده نمی‌کند.

درست نادرست

10 پرسش 10

10. آزمایش منظم روش‌های بازیابی داده بخش مهمی از بازیابی فاجعه است.

درست نادرست

ایستگاه بررسی 3: درج اصطلاح کلیدی

هر جملهٔ زیر را بخوانید و جای خالی را با واژهٔ درست از بانک واژگان پر کنید.

1. محروم کردن دسترسی به فایل‌های محلی از _____ رمزنگاشتی استفاده می‌کند.
2. کد مخرب فعالی که روی سیستم اجرا می‌شود، _____ است.
3. نسخه‌های ذخیرهٔ بیرونی و قطع‌شده، یک _____ امن را تشکیل می‌دهند.
4. جلوگیری از گسترش بدافزار مستلزم _____ شبکهٔ نقاط پایانی است.
5. پرداخت ارز دیجیتالی که مجرمان سایبری می‌خواهند، _____ است.
6. بازگرداندن فایل‌های داده عملیاتی، نمایانگر _____ پس از فاجعه است.

بانک واژگان

باج | بازیابی | پشتیبان سرد | تروجان | جداسازی | رمزگذاری | فاجعه | محموله

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم امنیت

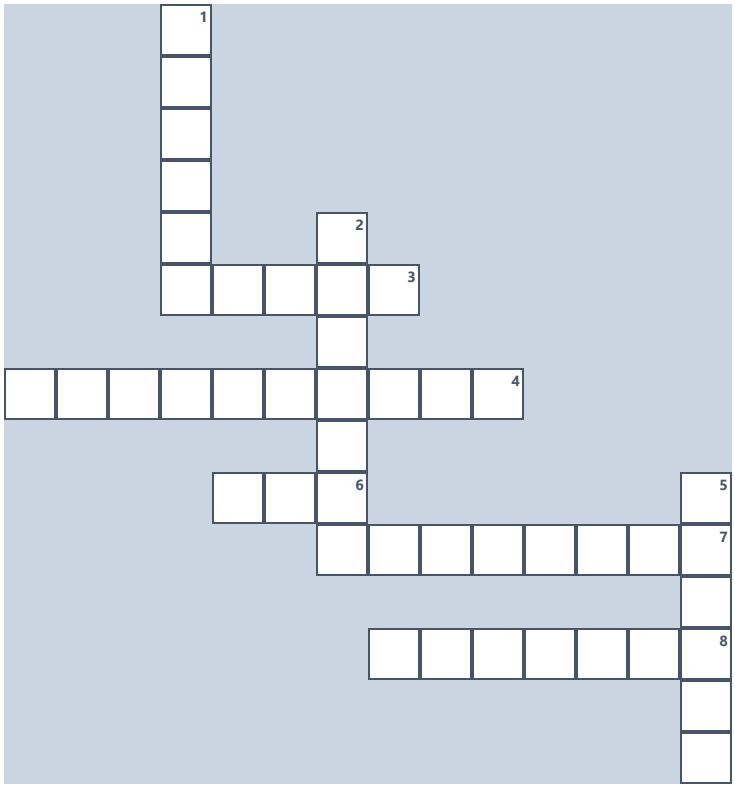
تطبیق تعاریف

هر اصطلاح واژگان در سمت راست را با نوشتن حرف متناظر (A-H) در کادر ورودی قابل‌پرکردن به تعریف درست آن در سمت چپ وصل کنید.

1. رمزگذاری	A	قطع اتصال سیستم‌های شبکهٔ آلوده.
2. بار داده	B	فایل مخرب که به‌صورت فایل سالم درآمده است.
3. پشتیبان سرد	C	قفل کردن رمزنگاری‌شدهٔ فایل‌ها.
4. جداسازی	D	رویداد اختلال عمدهٔ سیستم.
5. باج	E	اجرای نرم‌افزار مخرب.
6. بازیابی	F	نسخهٔ آفلاین جداشده.
7. فاجعه	G	بازیابی پایگاه داده از پشتیبان.
8. تروجان	H	درخواست پرداخت کلید رمزنگاری.

ایستگاه بررسی 5: جدول‌کلمات

جدول کلمات متقاطع را با تایپ حروف در خانه‌های سفید فعال حل کنید. شماره‌ها با سرنخ‌های زیر مطابقت دارند.



افقی

3. رویداد اختلال بزرگ در سامانه. (5)

4. نسخهٔ جداشده و آفلاین. (10)

6. درخواست پرداخت برای کلید رمزنگاری. (3)

7. قفل کردن فایل‌ها به روش رمزنگاشتی. (8)

8. قطع سامانه‌های آلودهٔ شبکه. (7)

عمودی

1. اجرای نرم‌افزار مخرب. (6)

2. برگرداندن پایگاه داده از نسخهٔ پشتیبان. (7)

5. فایل مخربی که سالم جلوه می‌کند. (6)

ایستگاه بررسی 5 – فعالیت جایگزین: سرنخ‌های دسترس‌پذیر جدول‌کلمات

کاربران صفحه‌خوان و صفحه‌کلید می‌توانند پاسخ‌های جدول کلمات متقاطع را مستقیماً در فیلدهای متنی زیر تایپ کنند.

افقی

3 افقی: رویداد اختلال بزرگ در سامانه. (5 حرف):

4 افقی: نسخهٔ جداشده و آفلاین. (10 حرف):

6 افقی: درخواست پرداخت برای کلید رمزنگاری. (3 حرف):

7 افقی: قفل کردن فایل‌ها به روش رمزنگاشتی. (8 حرف):

8 افقی: قطع سامانه‌های آلودهٔ شبکه. (7 حرف):

عمودی

1 عمودی: اجرای نرم‌افزار مخرب. (6 حرف):

2 عمودی: برگرداندن پایگاه داده از نسخهٔ پشتیبان. (7 حرف):

5 عمودی: فایل مخربی که سالم جلوه می‌کند. (6 حرف):

ایستگاه بررسی 6: جدول کلمات پنهان

8 اصطلاح کلیدی واژگان را که در جدول زیر پنهان شده‌اند پیدا کنید. کلمات می‌توانند افقی، عمودی یا مورب باشند.

ه	ظ	و	ح	ظ	س	ت	غ	ذ	ح	ص	غ	ش	ظ	ن
ع	ض	ه	ت	ک	ف	ق	ج	ب	ژ	ر	پ	ا	ب	پ
ط	و	ع	ژ	ز	و	ژ	ن	ک	ا	ز	ث	ع	ش	ر
ث	ذ	ج	ن	ا	چ	و	ر	ت	س	ز	ص	ژ	ع	ظ
خ	ش	ا	ش	ع	پ	غ	ف	ک	ک	خ	ی	پ	ف	ظ
ی	ض	ف	د	ف	ش	پ	ر	م	ث	ق	ه	ا	گ	ت
ز	ی	م	ح	ز	ت	خ	ی	م	ث	ص	ث	ع	ب	ن
ا	ظ	پ	گ	ب	ی	ا	ی	ح	ز	ض	ث	ژ	ا	ی
س	ث	ض	ث	چ	ب	خ	ذ	م	ث	گ	غ	ع	ش	چ
ا	ذ	ف	ی	ق	ا	چ	ع	و	ل	چ	ذ	ا	ا	ع
د	ط	ص	ظ	ک	ن	و	ع	ل	ز	غ	ک	ا	ف	ت
چ	ص	ه	پ	ح	س	ف	ن	ه	چ	م	ر	ا	ر	غ
ی	ه	ه	ژ	ح	ر	ذ	ش	ا	غ	ز	س	س	ق	ی
ط	خ	ظ	ع	خ	د	ی	ب	ا	ض	ل	ح	گ	پ	ه
ف	ه	ب	خ	س	ی	خ	ز	ض	ظ	ص	ن	پ	س	ی

فهرست واژگان

رمزگذاری
محموله
پشتیبانسرد
جداسازی
باج
بازیابی
فاجعه
تروجان

ایستگاه بررسی 6 – فعالیت جایگزین: تطبیق دسترس‌پذیر واژگان

هر یک از 8 اصطلاح واژگان موجود در جدول کلمات پنهان را با نوشتن حرف (A-H) در جای خالی به تعریف درست آن وصل کنید.

اصطلاحات واژگان	تعاریف و فیلدهای تطبیق
A. رمزگذاری	1. نسخهٔ جداشده و آفلاین.
B. محموله	2. فایل مخربی که سالم جلوه می‌کند.
C. پشتیبانسرد	3. قفل کردن فایل‌ها به روش رمزنگاشتی.
D. جداسازی	4. درخواست پرداخت برای کلید رمزنگاری.
E. باج	5. قطع سامانه‌های آلودهٔ شبکه.
F. بازیابی	6. رویداد اختلال بزرگ در سامانه.
G. فاجعه	7. اجرای نرم‌افزار مخرب.
H. تروجان	8. برگرداندن پایگاه داده از نسخهٔ پشتیبان.

ایستگاه بررسی 7: چالش کلمات درهم‌ریخته

حروف زیر را مرتب کنید تا مفاهیم و اصطلاحات کلیدی امنیت سایبری آشکار شوند. پاسخ‌هایتان را در کادرهای ورودی ارائه‌شده بنویسید.

1. ر گ ذ ر ا م ی ز
2. ر ی پ ش ب د ن س ا ت
3. ج ا ب
4. ج ه ع ف ا
5. و م ه م ل ح
6. ز ا ا ج س ی د
7. ب ب ا ی ا ی ز
8. و ن ت ا ج ر

فعالیت تکمیلی: سریع فکر کن

برای هر دسته 3 پاسخ بنویسید. هر کس زودتر فهرست را کامل کند برنده است.

1	اطلاعاتی که هرگز نباید به اشتراک بگذارید		
2	دستگاه‌هایی که می‌توانند هک شوند		
3	دلایل نپرداختن باج		
4	عادت‌های ایمن که می‌توانید از امروز شروع کنید		
5	ابزارهای امنیتی که می‌شناسید		
6	روش‌های محافظت از حساب‌هایتان		
7	نشانه‌های آلوده بودن رایانه		
8	جاهایی برای نگهداری پشتیبان		
9	فایل‌هایی که هرگز نمی‌خواهید از دست بدهید		
10	روش‌های انتشار باج‌افزار		
11	کارهایی که در ساعت اول حمله باید انجام داد		
12	افرادی که هنگام حمله باید با آن‌ها تماس گرفت		
13	چیزهایی که باج‌افزار می‌تواند قفل کند		
14	واژه‌های مرتبط با امنیت سایبری		
15	سازمان‌هایی که اغلب هدف قرار می‌گیرند		

ایستگاه بررسی 8: مطالعات موردی امنیت سایبری

مفاهیمی را که آموخته‌اید برای حل سناریوهای واقعی زیر به کار ببرید.

مطالعهٔ موردی 1: مهار بار باج‌افزار در سازمان



سناریو: یک شبکهٔ محلی سازمانی توسط باج‌افزار فعال نفوذ شده است. سرورهای فایل کلیدی شروع به نمایش پسوند فایل .locked کرده‌اند.

پرسش برای بحث: مراحل مهار را شرح دهید و پروتکل بازیابی داده را بیان کنید.

مطالعهٔ موردی 2: ارزیابی معماری‌های پشتیبان‌گیری آفلاین



سناریو: یک سازمان می‌خواهد راهبردی برای پشتیبان‌گیری از داده طراحی کند که ریسک به خطر افتادن پشتیبان‌ها را کاهش دهد، حتی اگر شبکهٔ محلی اصلی کاملاً توسط باج‌افزار ربوده شود.

پرسش برای بحث: یک سامانهٔ خزانهٔ امن ذخیره‌سازی پشتیبان آفلاین طراحی کنید.

ایستگاه بررسی 9: رمزگشایی

متخصص امنیت سایبری از دارایی‌های شبکه در برابر عوامل تهدید آنلاین محافظت می‌کند. از کلید حرف-به-عدد زیر استفاده کنید و با نوشتن حرف‌های متناظر در جاهای خالی، پیام را رمزگشایی کنید.

کلید رمزگذاری حرف به عدد

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

ر=12 ز=13 ژ=14 س=15 ش=16 ص=17 ض=18 ط=19 ظ=20 ع=21 غ=22

ف=23 ق=24 ک=25 گ=26 ل=27 م=28 ن=29 و=30 ه=31 ی=32

13	1		31	10	1	10		32	2	1	32	13	1	2

10	12	15		29	1	2	32	4	16	3

پیام رمزگشایی‌شده:

نکته: هر عدد نشان‌دهندهٔ یک حرف فارسی از کلید بالا است.

ایستگاه بررسی 10: پرسش‌های متداول امنیت سایبری – مقدماتی (بخش A)

پرسش‌ها و پاسخ‌های رایج دربارهٔ کاهش تهدیدهای آنلاین را مرور کنید.

Q1: باج‌افزار چیست؟

باج‌افزار نرم‌افزاری مخرب است که برای مسدود کردن دسترسی به سیستم‌ها یا فایل‌های رایانه تا زمان پرداخت مبلغ باج طراحی شده است.

Q2: باج‌افزار چگونه گسترش می‌یابد؟

از طریق پیوست‌های ایمیل فیشینگ، آسیب‌پذیری‌های نرم‌افزار بدون وصله و سامانه‌های دسترسی راه دور نفوذشده. [1]

Q3: چرا پرداخت به رمزارز درخواست می‌شود؟

رمزارزهایی مانند بیت‌کوین ناشناسی نسبی ارائه می‌دهند و ردیابی وجوه را برای نهادهای مجری قانون دشوار می‌کنند.

Q4: آیا آنتی‌ویروس باج‌افزار را مسدود می‌کند؟

بله، اما آنتی‌ویروس مبتنی بر امضا ممکن است در برابر بارهای آلودهٔ باج‌افزار روز صفر تازه‌ساخته‌شده شکست بخورد.

Q5: پشتیبان جداشده از شبکه (air-gapped) چیست؟

نسخهٔ پشتیبانی که هیچ ارتباط فیزیکی یا منطقی با شبکهٔ اصلی ندارد و از آن در برابر گسترش آلودگی محافظت می‌کند.

ایستگاه بررسی 10: پرسش‌های متداول امنیت سایبری – مقدماتی (بخش B)

پرسش‌ها و پاسخ‌های رایج دربارهٔ کاهش تهدیدهای آنلاین را مرور کنید.

Q6: دوگانه‌اخاذی چیست؟

زمانی که مهاجمان نه‌تنها فایل‌ها را رمزگذاری می‌کنند، بلکه داده‌های حساس را هم می‌دزدند تا در صورت پرداخت‌نشدن، تهدید به انتشار عمومی کنند.

Q7: رمزگشا (decryptor) چیست؟

ابزار نرم‌افزاری که شامل کلید رمزنگاری لازم برای بازگردانی فایل‌های قفل‌شده به متن ساده است.

Q8: باج‌افزار را چگونه زود تشخیص می‌دهید؟

با پایش سامانه‌های فایل برای فعالیت ناگهانی و گستردهٔ تغییر و تغییر نام فایل‌ها.

Q9: نقش بیمه چیست؟

بیمهٔ سایبری می‌تواند به پوشش هزینه‌های بازیابی کمک کند، اما شرایط پوشش و قوانین پرداخت باج بسته به بیمه‌نامه متفاوت است.

Q10: آیا باید سیستم آلوده را ریبوت کنم؟

خیر، راه‌اندازی مجدد می‌تواند شواهد حافظهٔ فرار را از بین ببرد؛ به‌جای آن، آن را از شبکه جدا کنید. [1]

ایستگاه بررسی 10: پرسش‌های متداول امنیت – پیشرفته (بخش C)

جنبه‌های فنی پیشرفتهٔ چارچوب‌های امنیتی، تحلیل بدافزار و انطباق داده را بررسی کنید.

Q1: باج‌افزار چگونه از رمزگذاری نامتقارن استفاده می‌کند؟

از یک کلید عمومی تعبیه‌شده در بدافزار برای رمزگذاری فایل‌ها استفاده می‌کند و برای رمزگشایی به کلید خصوصی مهاجم نیاز دارد.

Q2: چرا رمزگذاری متقارن نیز به کار می‌رود؟

رمزگذاری متقارن (مانند AES) سریع است و می‌تواند پایگاه‌های داده عظیم را در چند دقیقه قفل کند، در حالی که کلیدهای نامتقارن کلید AES را ایمن می‌کنند.

Q3: بخش‌بندی منطقی چیست؟

تقسیم شبکه‌ها به مناطق منزوی که از انتشار جانبی بدافزار از گره‌های ایستگاه کاری به سرورهای اصلی جلوگیری می‌کند.

Q4: ذخیره‌سازی WORM چیست؟

رسانهٔ یک‌بار-نوشتن، چندبار-خواندن (WORM) که مانع می‌شود داده‌های پشتیبان توسط بارهای آلودهٔ باج‌افزار ویرایش، بازنویسی یا حذف شوند.

Q5: نسخه‌های سایه (shadow copies) چیستند؟

نسخه‌های پشتیبان محلی که ویندوز می‌سازد؛ باج‌افزار معمولاً ابتدا آن‌ها را با ابزارهای مدیریتی حذف می‌کند.

ایستگاه بررسی 10: پرسش‌های متداول امنیت – پیشرفته (بخش D)

جنبه‌های فنی پیشرفتهٔ چارچوب‌های امنیتی، تحلیل بدافزار و انطباق داده را بررسی کنید.

Q6: سرقت اعتبارنامه چگونه باج‌افزار را ممکن می‌کند؟

مهاجمان نام‌کاربری و گذرواژهٔ مدیر لورفته را می‌خرند تا از طریق دسکتاپ‌های راه دور وارد شوند و باج‌افزار را به‌صورت دستی در سراسر شبکه اجرا کنند.

Q7: آزمون بازیابی آزمایشی (dry-run) چیست؟

بازیابی منظم پایگاه‌های داده پشتیبان در محیط‌های آزمایشی ایزوله تا مطمئن شویم سرعت بازیابی و یکپارچگی داده با معیارهای بازیابی فاجعه سازگار است.

Q8: تشخیص نقطهٔ پایانی (EDR) چگونه جلوی باج‌افزار را می‌گیرد؟

با تحلیل رفتار فرایند (مثلاً رمزگذاری سریع) و تعلیق سریع برنامهٔ سرکش.

Q9: مدل باج‌افزار به‌عنوان سرویس (RaaS) چیست؟

مدل فرانچایز که در آن توسعه‌دهندگان بدافزار سازندگان باج‌افزار را در ازای درصدی از پرداخت‌ها به همکاران اجاره می‌دهند.

Q10: RDP وصله‌نشده چگونه باج‌افزار را فعال می‌کند؟

دروازه‌های Remote Desktop Protocol در معرض دید و وصله‌نشده به مهاجمان اجازه می‌دهند ورودها را با حملهٔ آزمون‌وخطا بشکنند و بدافزار را به‌صورت دستی اجرا کنند.

بخش 11: 10 واقعیت و بینش دنیای واقعی دربارهٔ امنیت سایبری

واقعیت‌های دنیای واقعی دربارهٔ نقض‌های امنیتی، سازوکارهای دفاعی و استانداردهای انطباق را مرور کنید.

1. بینش امنیت

عوامل باج‌افزار اغلب از ابزارهایی مانند vssadmin.exe برای حذف نسخه‌های سایهٔ ویندوز و مسدود کردن بازیابی‌های محلی استفاده می‌کنند. [1]

2. بینش امنیت

کلیدهای متقارن AES-256 معمولاً برای رمزگذاری بار فایل‌ها استفاده می‌شوند و سپس با کلیدهای عمومی RSA قفل می‌شوند.

3. بینش امنیت

بازیابی پس از یک حملهٔ موفق باج‌افزار می‌تواند هفته‌ها طول بکشد؛ به همین دلیل پشتیبان‌های آفلاین آزمایش‌شده اهمیت دارند.

4. بینش امنیت

FBI از پرداخت باج حمایت نمی‌کند و هشدار می‌دهد که پرداخت، تضمین نمی‌کند داده‌هایتان را پس بگیرید. [2]

5. بینش امنیت

طرح‌های بازیابی پس از فاجعه (DRP) باید یک هدف زمان بازیابی (RTO) و یک هدف نقطهٔ بازیابی (RPO) تعریف کنند.

6. بینش امنیت

FBI پشتیبان‌گیری‌هایی را توصیه می‌کند که رمزگذاری‌شده و تغییرناپذیر باشند، یعنی نتوان آن‌ها را تغییر داد یا حذف کرد. [3]

7. بینش امنیت

توسعه‌دهندگان باج‌افزار از تکنیک‌های پیشرفتهٔ مبهم‌سازی برای دور زدن اسکنرهای آنتی‌ویروس سنتی مبتنی بر امضا استفاده می‌کنند.

8. بینش امنیت

بخش‌بندی شبکه حرکت جانبی را محدود می‌کند و کمک می‌کند باج‌افزار فراتر از نخستین میزبان آلوده پخش نشود. [3]

9. بینش امنیت

سرویس‌های راه دور در معرض دید و ضعیف‌ایمن‌شده مانند Remote Desktop Protocol (RDP) نقطهٔ ورود رایج باج‌افزار هستند. [1]

10. بینش امنیت

CISA توصیه می‌کند پشتیبان‌های رمزگذاری‌شده به‌صورت آفلاین نگهداری شوند، زیرا بسیاری از انواع باج‌افزار پشتیبان‌های در دسترس را جست‌وجو و حذف می‌کنند. [1]

منابع و مراجع فنی

راهنمای مطالعه و پازل‌های تعاملی از استانداردهای جهانی NIST، OWASP و انطباق با حریم خصوصی داده گردآوری شده‌اند.

منابع علمی و صنعتی

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

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

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

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

کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

1 پرسش 1 — پاسخ درست: **A**

نکتهٔ آموزشی

سازوکار اصلی حملهٔ باج‌افزار چیست؟ → رمزگذاری فایل‌های کاربر برای سلب دسترسی به سیستم

2 پرسش 2 — پاسخ درست: **A**

نکتهٔ آموزشی

پشتیبان آفلاین (سرد) چیست؟ → نسخهٔ ذخیره‌ای که از شبکه جدا شده تا از انتشار بدافزار محافظت شود

3 پرسش 3 — پاسخ درست: **A**

نکتهٔ آموزشی

تیم‌های امنیتی هنگام حملهٔ باج‌افزار چگونه باید سامانه‌های آلوده را جدا کنند؟ → فوراً کابل‌های شبکه را جدا کنید و رابط‌های بی‌سیم را غیرفعال کنید

4 پرسش 4 — پاسخ درست: **A**

نکتهٔ آموزشی

چرا نهادهای امنیتی توصیه می‌کنند خواسته‌های باج‌افزار پرداخت نشود؟ → پرداخت وجه مهاجمان را تشویق می‌کند و تحویل کلید رمزگشایی را تضمین نمی‌کند

5 پرسش 5 — پاسخ درست: **A**

نکتهٔ آموزشی

برنامهٔ بازیابی پس از فاجعه (DRP) چیست؟ → فرایندی ساختاریافته برای بازگرداندن عملیات و داده‌ها پس از نفوذ به سیستم

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 پرسش 6

پاسخ درست: درست

نکتهٔ آموزشی

بارهای باج‌افزار به‌راحتی می‌توانند به پشتیبان‌های آنلاین متصل به شبکه منتشر شوند.

7 پرسش 7

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: FBI هشدار می‌دهد پرداخت تضمین نمی‌کند هیچ دادهٔ شما بازگردانده شود.

8 پرسش 8

پاسخ درست: درست

نکتهٔ آموزشی

درست: CISA توصیه می‌کند میزبان‌های آلوده را جدا کنید یا شبکه را آفلاین کنید تا گسترش مهار شود.

9 پرسش 9

پاسخ درست: نادرست

نکتهٔ آموزشی

نادرست: باج‌افزار معمولاً فایل‌ها را با رمزهای متقارن سریع مانند AES رمزگذاری می‌کند.

10 پرسش 10

پاسخ درست: درست

نکتهٔ آموزشی

آزمایش منظم روش‌های بازیابی داده بخش مهمی از بازیابی فاجعه است.

کلیدهای واژگان و معیار نمره‌دهی

بارم‌بندی معلم: برای هر تطبیق درست (در مجموع 8 امتیاز) و اصطلاح بافتی (در مجموع 6 امتیاز) 1 امتیاز بدهید.

ایستگاه بررسی 4: کلید پاسخ – تطبیق مفاهیم

C 1. رمزگذاری	E 2. بار داده	F 3. پشتیبان سرد	A 4. جداسازی
H 5. باج	G 6. بازیابی	D 7. فاجعه	B 8. تروجان

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 رمزگذاری	2 محموله	3 پشتیبان سرد	4 جداسازی
5 باج	6 بازیابی		

ایستگاه بررسی 6 – فعالیت جایگزین: کلید پاسخ – تطبیق واژگان

1 C – پشتیبانسرد	2 H – تروجان	3 A – رمزگذاری	4 E – باج
5 D – جداسازی	6 G – فاجعه	7 B – محموله	8 F – بازیابی

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند رمزگذاری، بار داده و پشتیبان سرد را با کلمات خودشان توضیح دهند و برای هر کدام مثالی بزنند.

مطالعات موردی:
از دانش‌آموزان بخواهید پیشنهادهای خود را بر پایهٔ واقعیت‌های کاربرگ ارائه کنند، نه نظر شخصی.

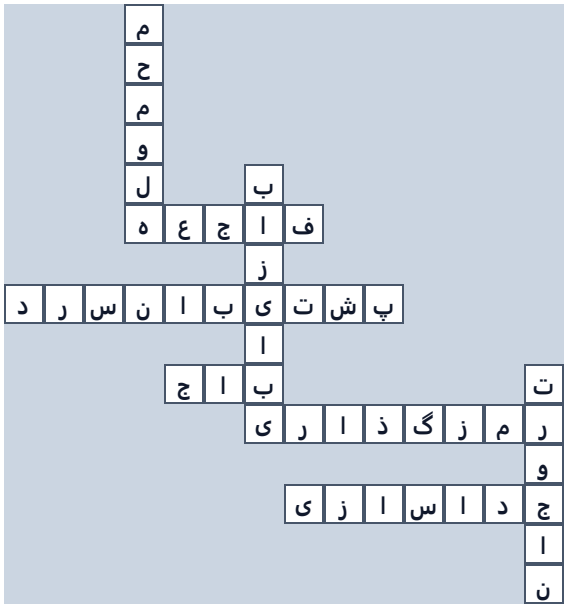
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

ه	ظ	و	ح	ظ	س	ت	غ	ذ	ح	ص	غ	ش	ظ	ن
ع	ض	ه	ت	ک	ف	ق	چ	ب	ژ	ر	پ	ا	ب	پ
ط	و	ع	ژ	ز	و	ژ	ن	ک	ا	ز	ث	ع	ش	ر
ث	ذ	چ	ن	ا	چ	و	ر	ت	ز	ص	ژ	ع	ظ	ظ
خ	ش	ا	ش	ع	پ	غ	ف	ک	ک	خ	ی	پ	ف	ظ
ی	ض	ف	د	ف	ش	پ	ر	م	ث	ق	ه	ا	گ	ت
ز	ی	م	ح	ز	ت	خ	ی	م	ث	ص	ث	ع	ب	ن
ا	ظ	پ	گ	ب	ی	ا	ی	ح	ز	ض	ث	ژ	ا	ی
س	ث	ض	ث	چ	ب	خ	ذ	م	ث	گ	غ	ع	ش	چ
ا	ذ	ف	ی	ق	ا	چ	ع	و	ل	ج	ذ	ا	ا	ع
د	ط	ص	ظ	ک	ن	و	ع	ل	ز	غ	ک	ا	ف	ت
چ	ص	ه	پ	ح	س	ف	ن	ه	چ	م	ر	ا	ر	غ
ی	ه	ه	ژ	ح	ر	ذ	ش	ا	غ	ز	س	ق	ی	ی
ط	خ	ظ	ع	خ	د	ی	ا	ض	ل	ح	گ	پ	ه	ه
ف	ه	ب	خ	س	ی	خ	ز	ض	ظ	ص	ن	پ	س	ی

پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

3 افقی: فاجعه رویداد اختلال بزرگ در سامانه. (5 حرف)

4 افقی: پشتیبانسرد نسخهٔ جداشده و آفلاین. (10 حرف)

6 افقی: باج درخواست پرداخت برای کلید رمزنگاری. (3 حرف)

7 افقی: رمزگذاری قفل کردن فایل‌ها به روش رمزنگاشتی. (8 حرف)

8 افقی: جداسازی قطع سامانه‌های آلودهٔ شبکه. (7 حرف)

عمودی

1 عمودی: محموله اجرای نرم‌افزار مخرب. (6 حرف)

2 عمودی: بازیابی برگرداندن پایگاه داده از نسخهٔ پشتیبان. (7 حرف)

5 عمودی: تروجان فایل مخربی که سالم جلوه می‌کند. (6 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. رگذرامیز	رمزگذاری	5. ومهملح	محموله
2. ریپشبدنسات	پشتیبانسرد	6. زااجسید	جداسازی
3. جاب	باج	7. بباياز	بازیابی
4. جهعفا	فاجعه	8. ونتاجر	تروجان

کلید چالش رمز مخفی

"بازیابی داده از پشتیبان سرد"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: مهار بار باج‌افزار در سازمان

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: شبکهٔ محلی یک شرکت توسط باج‌افزار فعال نفوذ شده است. سرورهای فایل کلیدی شروع به نمایش پسوندهای فایل .locked کرده‌اند.
- راهبرد و راه‌حل توصیه‌شده: همهٔ سرورهای آسیب‌دیده را از شبکهٔ محلی جدا کنید. نشست‌های مدیریتی فعال را پایان دهید. فایل‌های آسیب‌ندیده را از یک سامانهٔ پشتیبان آفلاین امن با قفل نوشتن بازیابی کنید.

B مطالعهٔ موردی 2: ارزیابی معماری‌های پشتیبان‌گیری آفلاین

پاسخ معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک سازمان می‌خواهد راهبرد پشتیبان‌گیری از داده‌ها را طوری طراحی کند که حتی اگر شبکهٔ محلی اصلی کاملاً توسط باج‌افزار ربوده شود، خطر در معرض خطر قرار گرفتن نسخه‌های پشتیبان کاهش یابد.
- راهبرد و راه‌حل پیشنهادی: ذخیره‌سازی یک‌بار-نوشتن-چندبار-خواندن (WORM) را پیاده کنید. با قطع سامانهٔ پشتیبان از همهٔ شبکه‌ها یک air-gap منطقی ایجاد کنید و چرخش روزانهٔ رسانهٔ فیزیکی را اعمال کنید.