
مفاهیم فریب سایبری
کاشف
مدیریت امن الکترونیکی
(سهامی خاص)
ارائه دهندگان: سید علی صموتی
سجاد طرهانی
واحد توسعه خدمات
دپارتمان پژوهش و نوآوری
شرکت مدیریت امن الکترونیکی کاشف
مهر 1404


بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ
کاشف
مدیریت امن الکترونیکی
(سهامی خاص)

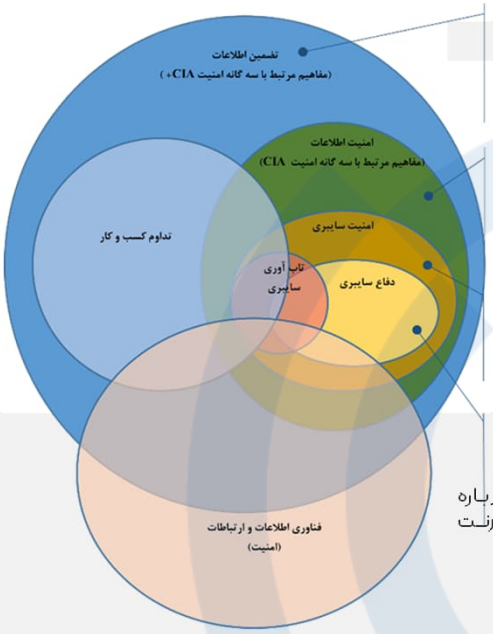
فصل اول

از دفاع سایبری تا تاب آوری سایبری

نکات مهم فصل:

- دفاع سایبری چیست؟
- تاب اوری سایبری چیست؟
- مفاهیم اولیه فریب

معرفی برخی از واژگان



تضمین اطلاعات

تدوین راهبرد/خط‌مشی برای کل رویکرد حفاظت از سیستم‌های اطلاعاتی و ارتباطاتی یا CIS، سیستم های غیر الکترونیک، هر شکلی از اطلاعات، و اینترنت (اشتراک حاکمیت و مدیریت مخاطرات).

امنیت سایبری

هر چیزی که مربوط به امنیت CIS، اطلاعات دیجیتالی و اینترنت باشد : محافظت کردن از فناوری، فرایند و افراد.

امنیت اطلاعات

هر چیزی که شامل امنیت CIS (پیاده سازی خط‌مشی، تضمین اطلاعات با بکارگیری آن توسط دارایی‌ها).

دفاع سایبری

هر چیزی که مربوط به دفاع درباره CIS یا اطلاعات دیجیتالی و اینترنت باشد : فناوری، فرایند و افراد.

آشنایی با برخی واژگان از دید ناتو

1 تضمین اطلاعات	تأمین محرمانگی، یکپارچگی و دسترس‌پذیری؛ شامل اقدامات محافظتی و دفاعی.
2 امنیت اطلاعات	تمرکز بر تداوم کسب‌وکار و کاهش آسیب‌ها؛ پیاده‌سازی معیارهای امنیتی؛ مسئولیت محافظت از اطلاعات در برابر تهدیدات بر اساس مدل CIA .
3 امنیت سایبری	تأکید بر جلوگیری از دسترسی غیرمجاز و مقابله با تهدیدات سایبری.
4 دفاع سایبری	شامل اقدامات فعال و غیرفعال؛ هدف حفاظت از داده‌ها در برابر تهدیدات سایبری.

۶

آشنایی با برخی واژگان

5 **تاب‌آوری سایبری**

تأکید بر تداوم کسب‌وکار و امنیت اطلاعات؛ تفاوت با امنیت سایبری در تمرکز بر واکنش به تهدیدات.

6 **تهاجم سایبری**

شناسایی عاملان این تهدیدات به‌دلیل ماهیت غیرنظامی دشوار است.

۷

ماکت پلیس را همه دیده ایم

فقط ماکت ماشین پلیس.

ماکت ماشین پلیس و ماکت خود پلیس.

ماکت ماشین پلیس + دوربین سرعت سنج در همان مکان .

ماکت ماشین پلیس + دوربین سرعت سنج کمی دورتر.

۸

ارتباط تاب آوری سایبری و فریب .....

تاب‌آوری سایبری توانایی یک سیستم یا سازمان برای **مقاومت**، **تطبیق** و **بازیابی سریع** در برابر حملات سایبری، خرابی‌ها یا اختلالات است. در حوزه فریب از فناوری‌هایی استفاده می‌شود تا مهاجمان را گمراه کرده و با کاهش سطح حمله، تاب‌آوری سیستم را تقویت کند.

گمراه کنندگی
آیا مهاجم را فقط گمراه کنیم ؟

تطبیق
سیستم را بر اساس مهاجمان تطبیق دهیم .

بازیابی سریع
بر اساس گزارشات بتوان بازیابی سریع را انجام داد.

۹

اهداف تاب‌آوری سایبری بر اساس سند NIST 800-160

پیش‌بینی
حفظ وضعیت آمادگی آگاهانه برای شرایط نامطلوب.

بازیابی
بازیابی مأموریت یا عملکردهای تجاری در طول یا پس از شرایط نامطلوب.

مقاومت
ادامه‌دادن به مأموریت ضروری و وظایف تجاری با وجود شرایط نامطلوب.

سازگاری
تغییر مأموریت یا عملکردهای تجاری و/یا قابلیت‌های پشتیبانی به تغییرات پیش‌بینی‌شده در محیط‌های فنی، عملیاتی یا تهدید.

۱۰

بررسی سند NIST 800-160

تاب‌آوری سایبری توانایی پیش‌بینی، مقاومت، بازیابی و انطباق با شرایط نامطلوب، تنش ها، حملات یا مخاطرات سامانه‌هایی است که از منابع سایبری استفاده می‌کنند یا توسط آن‌ها فعال می‌شوند.

NIST 800-160

در نوامبر سال 2016 میلادی منتشر شد - سازمان‌ها چگونه می‌توانند سامانه‌های امن را طراحی، توسعه و استقرار دهند به‌طوری که قابل اعتماد بوده و در برابر مهاجمان مقاوم باشند.

NIST 800-160 Vol. 1

راهنمایی در مورد مهندسی امنیت سامانه‌ها با تأکید بر محافظت در برابر فقدان دارایی را ارائه می‌دهد.
علاوه بر امنیت، سایر جنبه‌های قابلیت اعتماد عبارتند از قابلیت اطمینان، ایمنی، تاب‌آوری و حفظ حریم خصوصی.

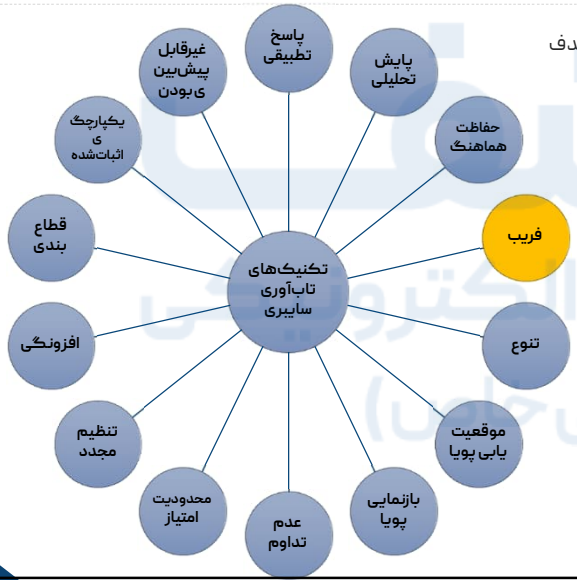
NIST 800-160 Vol. 2

بر ویژگی تاب‌آوری سایبری تمرکز دارد که رابطه قوی با امنیت و مقاومت دارد.

۱۱

تکنیک‌های تاب‌آوری سایبری

مجموعه‌ای از فناوری‌ها و فرایندهایی که برای دستیابی به یک یا چند هدف در نظر گرفته شده است.



۱۲

فصل دوم

مفـاهیم فریـــب ســایبری و المان ها

نکات مهم فصل:

- تعریف فریب
- انواع فریب
- چرخه عمر فریب

مروری بر برخی از تعاریف فریب

فریب سایبری در مستندات مختلف به صور متفاوت تعریف شده است:

1 تعریف 1

فریـب سـایبری بـه مجموعـه‌ای از روش‌هـا و فنـون اشاره دارد کـه باهـدف گـمـراه کـردن مهاجمـان از فعالیت‌هایشـان در شـبکه‌ها به‌کار گرفته می‌شود.

2 تعریف 2

فریب سایبری با جمع‌آوری و تحلیل اطلاعات مربـوط بـه الگوهـای حملـه، بـه سـازمان‌ها کمک می‌کنند تا دفاع‌های خود را در برابر تهدیدات تقویت نمایند.

3 تعریف 3

یک راهبرد پیشگیرانه، بر اساس منحـرف کـردن توجه مهاجمان و ایجاد سردرگمی در میان آن‌ها بنا شده است.

4 تعریف 4

کـه فریـب سـایبری بـه‌عنوان ابـزاری مـؤثر در تقویـت بازدارنـدگی در برابـر تهدیـدات تـرکیبی اسـت و بـه سازمان‌ها ایـن امکـان را می‌دهـد کـه بـا کـاهش نـرخ کاذب شناسایی تهدیدات، بـه طـور مـؤثرتر از داده‌هـا و زیرساخت‌های خود حفاظت کنند.

۱۴

یک روش کلی تقسیم بندی فریب

فریب به دودسته اصلی تقسیم می‌شود: فریب آشکار و فریب پنهان.

فریب آشکار،

جایی است که کاربران خودی از وجود فریب مطلع هستند و می‌توانند با احتیاط بیشتری عمل کنند. فریب آشکار می‌تواند شفافیت و اعتماد را افزایش دهد، اما می‌تواند مانع رفتارهای پرخطر کاربران شود.

فریب پنهان

کاربران خودی از وجود فریب بی‌خبرند و به طور طبیعی عمل می‌کنند. فریب پنهان می‌تواند اطلاعات مفیدی درباره حمله‌کنندگان جمع‌آوری کند، اما ممکن است به اعتماد کاربران آسیب بزند.

تعریف کلی

در پژوهش ها به صورت ممکن فریب را طبقه بندی میکنند که به برخی در این گفتار اشاره شده است.

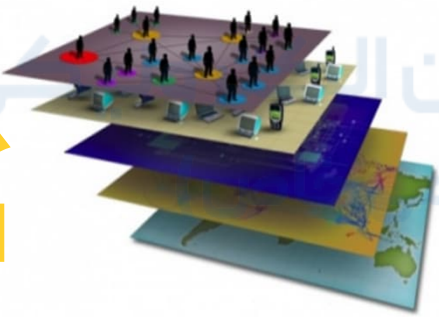
۱۵

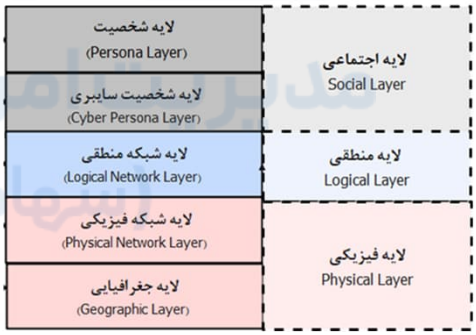
یک روش کلی تقسیم‌بندی فریب

مراحل فریب شامل راهبرد، بُعد، مرحله ، تکنیک و تاکتیک است.
راهبرد، به استفاده از فریب سایبری برای حمله یا دفاع اشاره دارد؛ حمله با فریب، راهکنشی. پیچیده است که مجرمان سایبری برای نفوذ به سامانه‌ها و دسترسی غیرمجاز به اطلاعات حساس از آن استفاده می‌کنند.
درحالی‌که دفاع با فریب یک راهبرد پیشگیرانه یا واکنشی. برای محافظت در برابر تهدیدهای سایبری است.

بُعد فریب

بُعد مشخص می‌کند که فریب در کدام بخش (داده، شبکه، سامانه یا نرم‌افزار) استفاده می‌شود تا مهاجمان را گمراه کند یا مدافعان را تقویت کند.





۱۶

تمایز محیط واقعی و غیر واقعی

فنـاوری فریـب میزبان‌هـای محاسـباتی فریبنـده و دسـتگاه‌های شبکه‌ای را فراهم می‌کند مانند دارایی واقعی است و از دارایی‌های تولید متمایز نیستند.

یک مهاجم اغلب نمی‌تواند ماهیت واقعی دارایی‌های فریبنده را بدون بررسی دقیق‌تر تعیین کند.

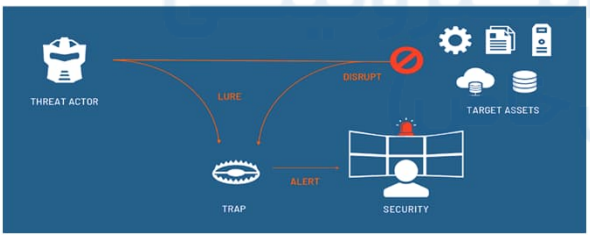
فناوری فریب هرگونه تلاش فعال برای مشاهده این دستگاه‌ها یا کسب اطلاعات از آن‌ها را تشخیص می‌دهد و یک هشدار با سطح اطمینان بالا به تیم واکنش به حادثه ارسال می‌کند.

۱۷

تمایز محیط واقعی و غیر واقعی

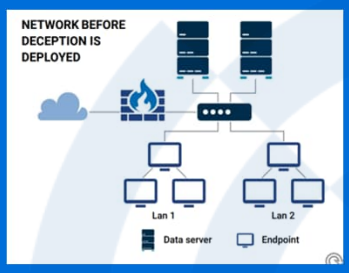
فناوری فریب مدرن تمرکز فریب را فراتر از هانی‌پات به نقطه پایانی، کارگزار و دستگاه منتقل می‌کند.

با درج اعتبارنامه‌های فریبنده در میزبان یا رهگیری تلاش‌های مهاجم برای استفاده از سامانه‌های احراز هویت شبکه مانند اکتیو دایرکتوری، تیم امنیت اطلاعات بینش و دید ارزشمندی را از فعالیت‌های مهاجم به دست می‌آورد درحالی‌که کار را برای یک عامل مخرب بسیار پیچیده‌تر می‌کند.



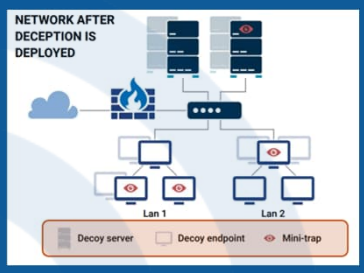
۱۸

شمای کلی یک شبکه قبل و بعد از استقرار فناوری فریب سایبری



نمای شبکه قبل استقرار فریب

شبکه بدون طعمه می باشد.



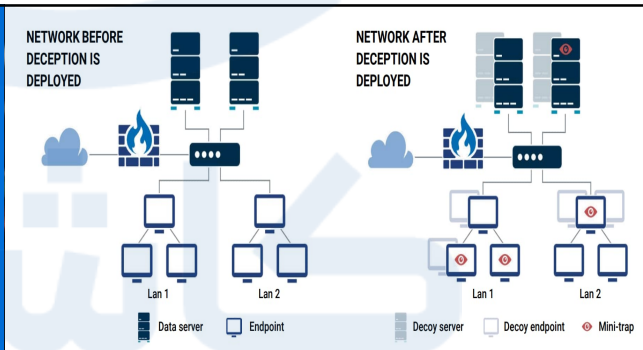
نمای شبکه بعد استقرار فریب

طعمه ها در کل شبکه وجود دارند.

۱۹

شمای کلی یک شبکه قبل و بعد از استقرار فناوری فریب سایبری

در شکل ها فناوری فریب دقیقا مانند دارایی اصلی عمل میکند مانند یک دیتا یس یا شبکه یا .....



عدم امکان تعیین واقعی یا غیر واقعی

یک مهاجم اغلب نمی‌تواند ماهیت واقعی دارایی‌های فریبنده را بدون بررسی دقیق‌تر تعیین کند.

شناسایی تلاش برای دستیابی به طعمه

فناوری فریب هرگونه تلاش فعال برای مشاهده این دستگاه‌ها یا کسب اطلاعات از آن‌ها را تشخیص می‌دهد و هشدار...

توسعه فعالیت

فناوری فریب مدرن تمرکز فریب را فراتر از هانی‌پات به نقطه پایانی، سرور و دستگاه منتقل می‌کند.

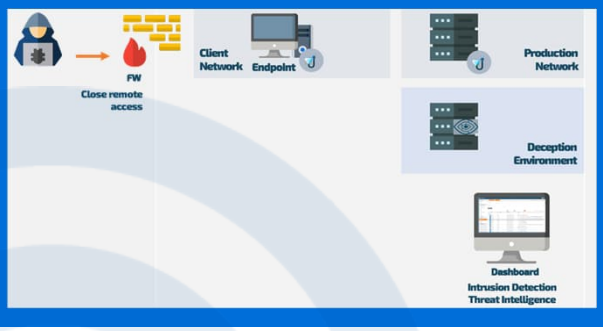
بینش ارزشمند

با درج اعتبارنامه‌های فریبنده رهگیری تلاش‌های مهاجم برای استفاده از سامانه‌های احراز هویت شبکه تیم امنیت اطلاعات بینش و دید ارزشمندی را از فعالیت‌های مهاجم به دست می‌آورد.

۲۰

فریب سایبری

جمع اوری داده های مهاجم از طریق طعمه ها



- نظارت بر شبکه
- بررسی دقیق رویداد
- بررسی دقیق رخداد
- مشاهده مقاصد و مسیر ها

۲۱

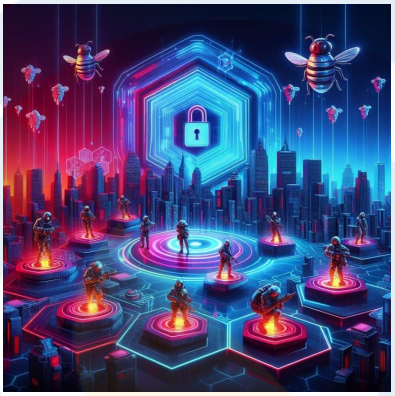
فناوری فریب در مقابل سایر فناوری‌های دفاع سایبری

مقایسه فریب و دفاع

عدم شناسایی حملات پیشرفته	مثبت کاذب بالا در دفاع	شناسایی حمله و مدیریت	شناسایی تهدیدات مشکوک و ناشناخته
راه‌حل‌های رایج دفاع سایبری اغلب قادر به تشخیص حملات پیشرفته نیستند.	این راه‌حل‌ها مثبت نادرست‌های زیادی تولید می‌کنند که زمان مدیران را مصرف می‌کند و آن‌ها را از خطر واقعی دور می‌کند.	فناوری فریب قادر است با فریب دادن مهاجمان حمله را شناسایی و مدیریت کند.	فناوری فریب قادر است تهدیدات ناشناخته را تشخیص داده، تحلیل کرده و با آن‌ها مقابله کنند.

۲۲

چرایی فریب - **مقایسه و مزایا**



- شناسایی سریع مهاجمان با نرخ مثبت نادرست پایین.
- کاهش آسیب‌های ناشی از مخاطره ناشی از حواس‌پرتی و/یا به تعویق انداختن اقدامات دفاعی.
- بازدارندگی مهاجم قبل از وقوع حمله یا قبل از وقوع آسیب قابل توجه.
- جمع‌آوری هوش تهدید خاص محیط.
- دستکاری و درگیری فعال مهاجم، به مدافع انسانی اجازه می‌دهد تا در زمان واقعی با مهاجم انسانی مقابله کند.
- .....

۲۳

حوزه‌های فریب سایبری

می توان حوزه های فریب سایبری را به صورت زیر طبقه بندی کرد.

۲۴

زیر مجموعه‌های فریب سایبری

پوشاندن
Masking

پنهان‌کردن داده‌ها یا اطلاعات حساس به‌گونه‌ای که غیرقابل‌کشف شوند.

منحرف‌کردن (طعمه‌گذاری)
Decoying

استفاده از اشیای جعلی برای جلب‌توجه مهاجمان از اهداف واقعی.

خلق یا اختراع
Inventing

طراحی و ایجاد موجودیت‌ها یا اطلاعات غیرواقعی، اما ظاهراً معتبر، به‌منظور فریب و گمراه‌سازی مهاجمان سایبری باهدف حفاظت از سامانه‌های اطلاعاتی.

تقلید
Mimicking

ایجاد موجودیت‌های جعلی که رفتار یا ظاهر سامانه واقعی را شبیه‌سازی می‌کنند.

25

زیر مجموعه‌های فریب سایبری

بسته‌بندی مجدد
Repackaging

تغییر ظاهر یا ویژگی‌های داده‌ها برای به‌نظرآمدن به‌عنوان چیزی دیگر.

پیشگیری

استفاده از فنونی مانند استگانوگرافی برای جلوگیری از حملات سایبری.

تحیرآفرینی

ایجاد ابهام و سردرگمی در مهاجمان برای دشوار کردن تشخیص حقیقت و بسیار واقعی جلوه دادن.

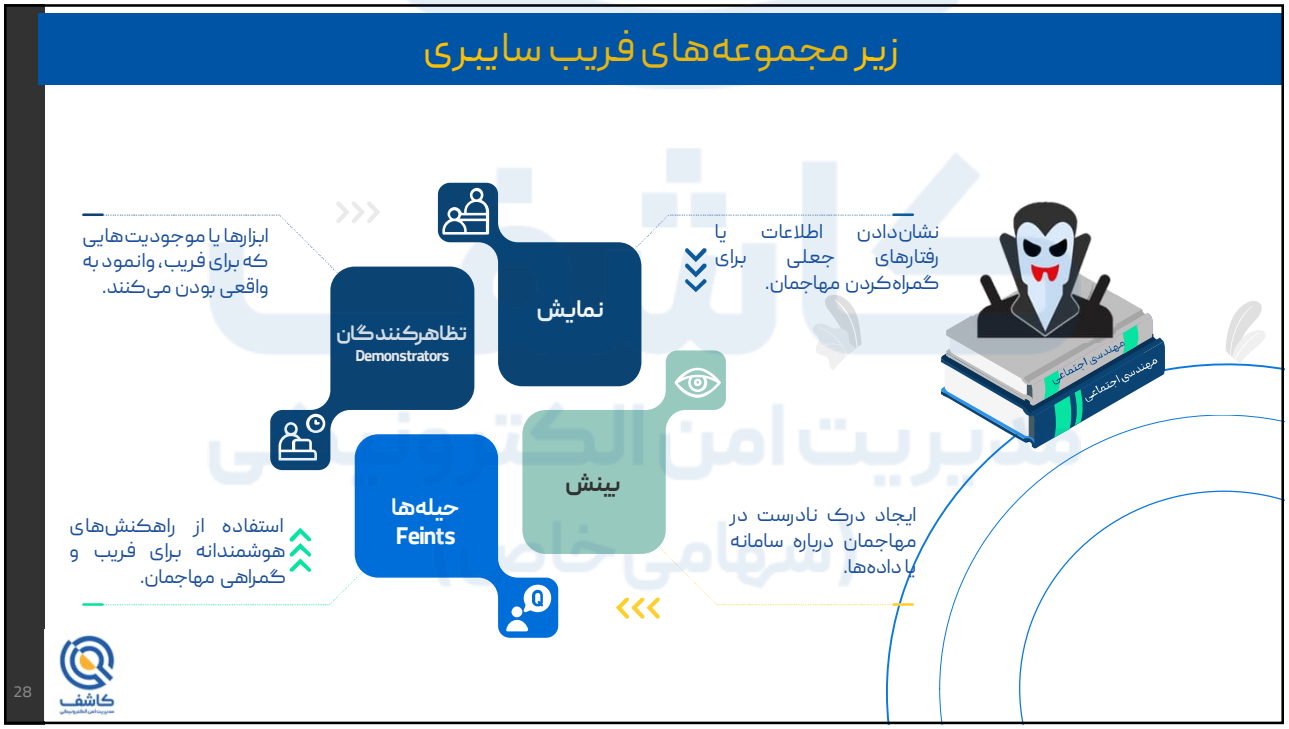
شبیه‌سازی

نمایش اطلاعات جعلی برای فریب مهاجمان و انحراف توجه آن‌ها.

26

زیر مجموعه‌های فریب سایبری

زیر مجموعه‌های فریب سایبری



زیر مجموعه‌های فریب سایبری

استفاده از راهبردهای فریب مشابه راهکنش‌های نظامی در امنیت سایبری.

حیله‌های جنگی Ruses

تکنیکی برای تصادفی کردن آدرس‌های حافظه جهت کاهش آسیب‌پذیری.

تصادفی‌سازی فضای آدرس Address Space Layout Randomization (ASLR)

نهان‌نگاری یا استتار یا استگانوگرافی

مخفی‌کردن داده‌ها در اشیای به‌ظاهر بی‌ضرر برای جلوگیری از تشخیص.

29

برخی از ابزار فریب سایبری

تکنیک	توضیحات	مزایا	چالش‌ها	کاربرد
تله‌های عسل	سامانه‌های فریب که به‌منظور جذب حمله‌کنندگان و جمع‌آوری اطلاعات در مورد روش‌ها و ابزارهای آن‌ها طراحی شده‌اند.	ارائه بینش عمیق درباره رفتار و راهکنش‌های حمله‌کنندگان؛ نرخ مثبت کاذب پایین؛ قابلیت شناسایی تهدیدات جدید.	نیاز به نظارت مداوم؛ ممکن است توسط حمله‌کنندگان ماهر شناسایی و دور زده شوند؛ هزینه‌های نگهداری بالا.	شناسایی حملات شبکه‌ای، تحلیل تهدیدات پیشرفته.
توکن‌های عسلی	داده‌ها یا اعتبارنامه‌های جعلی که در صورت دسترسی غیرمجاز، مدافعان را از نفوذ احتمالی مطلع می‌کنند.	آسان برای پیاده‌سازی و مدیریت؛ مفید برای شناسایی زودهنگام نفوذ؛ هزینه کم.	اثربخشی محدود اگر به طور راهبردی قرار نگیرند؛ ممکن است توسط مهاجمان نادیده گرفته شوند.	تشخیص نفوذ در پایگاه‌های داده، حفاظت از اطلاعات حساس.
دفاع‌های متحرک	فنونی که با تغییر مداوم پیکربندی سامانه‌ها، محیطی غیرقابل‌پیش‌بینی برای مهاجمان ایجاد می‌کنند.	افزایش پیچیدگی برای مهاجمان؛ کاهش احتمال شناسایی و نفوذ موفق؛ تقویت امنیت کلی سامانه.	نیاز به منابع محاسباتی بالا؛ ممکن است بر عملکرد سامانه‌های واقعی تأثیر منفی بگذارد.	حفاظت از زیرساخت‌های حیاتی، دفاع در برابر حملات تهدید مانای پیشرفته .

برخی از ابزار فریب سایبری

تکنیک	توضیحات	مزایا	چالش‌ها	کاربرد
فریب‌های دوطرفه	فنونی که اطلاعات نادرست را هم به مهاجمان و هم به مدافعان ارائه می‌دهند تا اعتماد مهاجمان را مختل کنند.	می‌تواند اعتماد مهاجمان به اطلاعات به‌دست‌آمده را کاهش دهد؛ ایجاد سردرگمی در راهکنش‌های مهاجم.	نیاز به طراحی بسیار دقیق؛ پیش‌بینی رفتار مهاجمان دشوار است؛ خطر تأثیر بر عملیات داخلی.	عملیات فریب پیشرفته، دفاع در برابر جاسوسی سایبری.
طعمه‌ها	سامانه‌ها یا خدمات جعلی که برای منحرف‌کردن مهاجمان از دارایی‌های واقعی طراحی شده‌اند.	محافظت از دارایی‌های واقعی؛ کاهش خطر حملات موفق؛ جمع‌آوری اطلاعات در مورد مهاجمان.	ممکن است توسط مهاجمان حرفه‌ای شناسایی شوند؛ نیاز به طراحی واقعی و جذاب برای فریب.	حفاظت از سرورها و سامانه‌های حساس، تحلیل رفتار مهاجم.

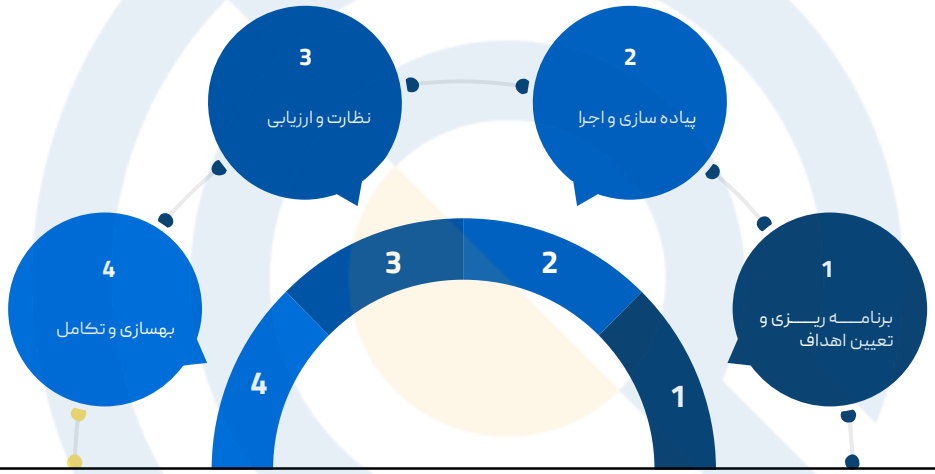
۳۱

روش های خلق فریب

۳۲

چرخه عمر فریب

مراحلی برای فریب تعریف شده است. مدل فریب یک‌دوره‌ای شامل 4 مرحله اصلی است:



۳۳

فصل سوم

تفاوت فریب با هانی پات

نکات مهم فصل:

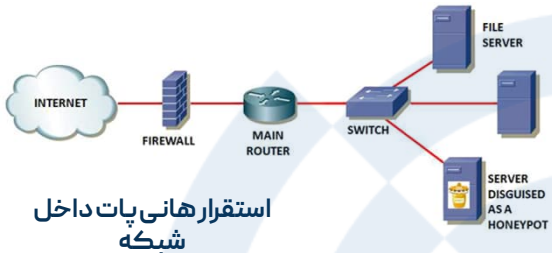
- انواع هانی پات ها
- تفاوت بنیادین مهندسی فریب با هانی پات

هانی‌پات

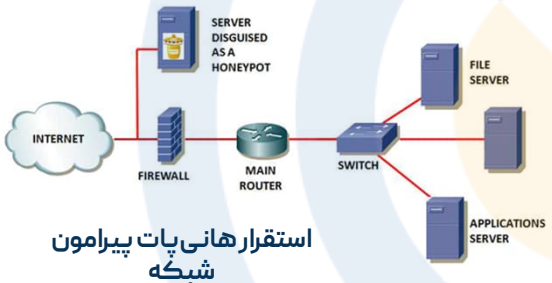
هانی‌پات‌ها اولین شکل از فناوری فریب سایبری بودند.

هانی‌پات‌های اولیه و فناوری فریب سایبری مدرن، هر دو بر ایجاد تله برای مهاجمان متکی هستند.

هانی‌پات‌های اولیه عمدتاً برای **پژوهش در زمینه تحلیل تهدیدات شبکه** استفاده می‌شدند و برای راه‌اندازی، نگهداری و تحلیل به منابع زیادی نیاز داشتند.



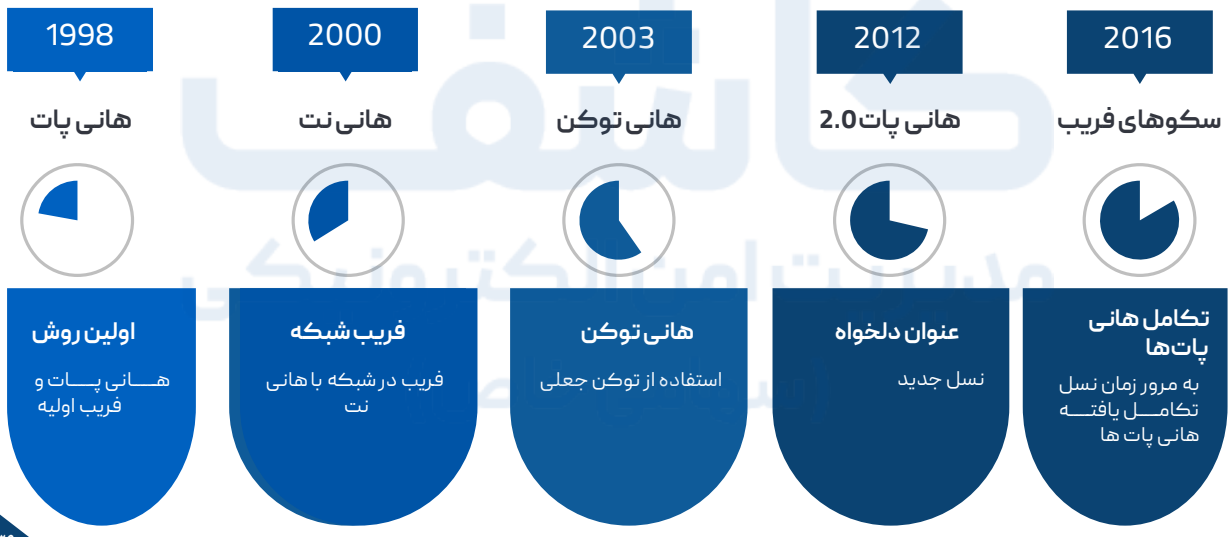
استقرار هانی‌پات داخل شبکه



استقرار هانی‌پات پیرامون شبکه

۳۵

نمودار تکامل هانی‌پات‌ها



۳۶

پیشرفت‌ها در فناوری فریب

اصالت

فناوری فریب از سیستم‌عامل، خدمات و برنامه‌های کاربردی برای ایجاد محیطی استفاده می‌کند که در آن طعمه‌ها برای مهاجم قابل شناسایی نیستند.

استقرار

فناوری فریب پیشرفته گزینه‌های انعطاف‌پذیری برای استقرار ارائه می‌دهد و از یادگیری ماشین برای یادگیری فعالیت‌های شبکه و آماده‌سازی فریب‌های معتبر استفاده می‌کند.

سهولت عملیات

سکوهای فریب مدرن از طریق یک کنسول مرکزی داخلی یا ابری به‌راحتی قابل استفاده و مدیریت هستند و برای کار یا نگهداری نیازی به تحلیلگران امنیتی بسیار ماهر ندارند.

محدودسازی حمله

سکوهای فریب مانع از استفاده مهاجم از فریب‌ها به‌عنوان پایگاهی برای حمله به بقیه محیط می‌شوند.

تعامل

سکوهای فریب با استفاده از فریب‌های با سطح تعامل بالا می‌توانند اطلاعات گسترده مهاجم را در طول تعامل جمع‌آوری کنند
این اطلاعات گزارش‌های **جرم‌یابی** را ارائه می‌دهند و فعالیت **پاسخ خودکار به حادثه** را فعال می‌کنند.

مقیاس‌پذیری

سکوهای فریب می‌توانند **به‌صورت سراسری** در محیط‌های فیزیکی، مجازی و ابری مستقر شوند.

۳۷

انواع تله های عسل

نام فارسی	نام انگلیسی	توضیحات
تله‌های عسل فیزیکی	Physical Honeypots	بر روی ماشین‌های جداگانه با آدرس IP منحصربه‌فرد پیاده‌سازی می‌شوند.
تله‌های عسل مجازی	Virtual Honeypots	بر روی یک سرور فیزیکی می‌توانند چندین نمونه را میزبانی کنند و از نظر هزینه و زمان به‌صرفه‌تر هستند.
تله‌های عسل غیرفعال	Passive Honeypots	به جمع‌آوری اطلاعات **بدون جذب مهاجمین** می‌پردازند.
تله‌های عسل فعال	Active Honeypots	به طور فعال سعی در فریب مهاجمین دارند.
تله‌های عسل خالص	Pure Honeypots	نسخه‌ای کامل از سامانه‌های واقعی با داده‌های جعلی هستند که مهاجمان را فریب می‌دهند.

۳۸

انواع تله های عسل

نام فارسی	نام انگلیسی	توضیحات
تله‌های عسل کم تعامل	Low-Interaction Honeypots	خدمات محدودی را شبیه‌سازی کرده و برای شناسایی حملات ساده با منابع کم مناسب‌اند.
تله‌های عسل پرتعامل	High-Interaction Honeypots	سامانه‌های پیچیده‌تری را شبیه‌سازی می‌کنند که امکان تعامل گسترده‌تر با مهاجمان را فراهم می‌کنند.
تله‌های عسل بدافزار	Malware Honeypots	برای جذب و تحلیل بدافزارها طراحی شده‌اند.
تله‌های عسل ایمیل	Email Honeypots	حساب‌های پست الکترونیک جعلی را برای شناسایی اسپم و حملات فیشینگ شبیه‌سازی می‌کنند.
تله‌های عسل اسپم	Spam Honeypots	برای جمع‌آوری و تحلیل ایمیل‌های هرزنامه استفاده می‌شوند.
تله‌های عسل عنکبوتی	Spider Honeypots	برای شناسایی خزنده‌های مخرب وب طراحی شده‌اند.
تله‌های عسل پایگاه داده	Database Honeypots	پایگاه‌های داده جعلی را برای جذب حملات به داده‌های حساس شبیه‌سازی می‌کنند.

۳۹

فصل چهارم

فریب و ارتباط با زنجیره کشتار و مایتره

نکات مهم فصل:

- مفاهیم زنجیره کشتار
- مایتره از دید دفاع و حمله
- ارتباط فریب و زنجیره کشتار

MITRE ATT&CK

مقابله با APT

تمرکز اصلی تاب‌آوری سایبری، مقابله با حملات APT است.

استفاده از رویکرد مایتره

با استفاده از چارچوب MITRE ATT&CK برای دسته‌بندی فعالیت‌های دشمن، روی رویدادهای تهدید تأثیر بگذارند.

ترکیب تاب‌اوری و تهدید

یکی از راه‌های درک بهتر نحوه انجام این کار، ترکیب چارچوب مهندسی تاب‌آوری سایبری با طبقه‌بندی رویدادهای تهدید است.

استفاده از رویکرد مایتره و دفاع

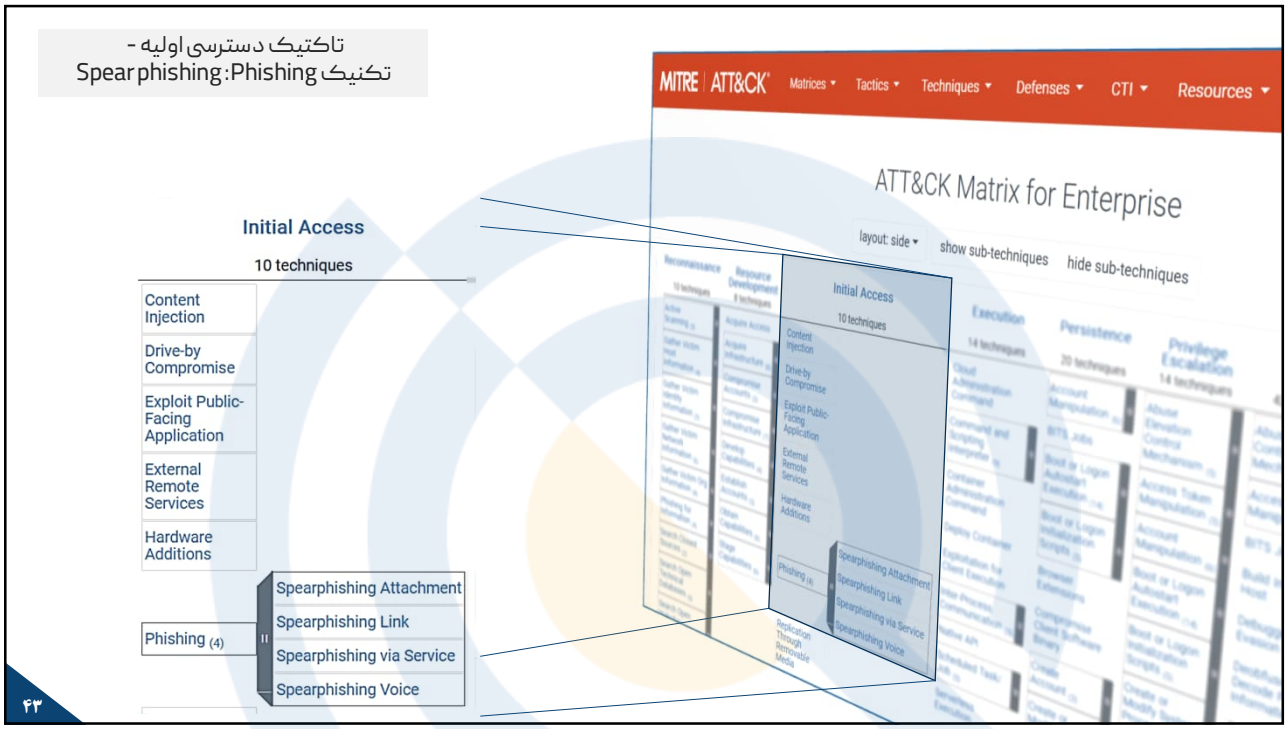
روش جدید دفاع مایتره هم در نظر گرفته شود.

نگاشت مایتره و لایه های فریب

مرحله حمله (عنوان فارسی)	مرحله حمله (عنوان لاتین)	توضیحات	لایه فریب شبکه	لایه فریب سامانه	لایه فریب نرم‌افزار	لایه فریب داده
شناسایی	Reconnaissance	جمع‌آوری اطلاعات از منابع باز، بررسی سامانه داخلی/شبکه، یا شنود ترافیک شبکه	✓	✓	✓	✓
تحویل	Delivery	ارسال بدافزار سفارشی از طریق ایمیل، وب‌سایت‌ها یا رسانه‌های قابل حمل	✓	✓	✓	
فرار از دفاع	Defense Evasion	غیرفعال کردن ابزارهای امنیتی، سوءاستفاده از فرایندهای معتبر، رمزنگاری و غیره	✓	✓	✓	
بهره‌برداری	Exploitation	بهره‌برداری از آسیب‌پذیری‌ها یا سهل‌انگاری کاربر برای پیشبرد مرحله‌های زنجیره	✓	✓	✓	
نصب	Installation	رهاکردن بدافزار و نصب تروجان دسترسی از راه دور یا بک‌در برای حفظ حضور		✓		
کنترل و فرماندهی	C2	برقراری ارتباط خروجی برای دریافت دستورات یا بارهای اضافی از مهاجم	✓	✓		
ارتقای امتیاز	Privilege Escalation	ارتقا دسترسی به‌صورت افقی یا عمودی برای دسترسی به دارایی‌های حساس		✓	✓	
دسترسی به اعتبارها	Credential Access	سرقت اعتبارنامه‌ها مانند نام کاربری و رمز عبور		✓	✓	✓
حرکت جانبی	Lateral Movement	جابه‌جایی در شبکه با استفاده از ابزارهای دسترسی از راه دور یا اعتبارهای سرقت‌شده	✓	✓	✓	✓
جمع‌آوری	Collection	جمع‌آوری داده‌های موردنظر از پایگاه‌داده، سامانه فایل، یا ورودی کاربر و غیره	✓	✓	✓	✓
خروج داده‌ها	Exfiltration	پردازش داده‌های جمع‌آوری‌شده و ارسال آن از طریق کانال C2 یا سایر کانال‌ها	✓	✓		

۴۲

تاکتیک دسترسی اولیه -
تکنیک Spear phishing:Phishing



فصل پنجم

معرفی برخی از پلت فرم های فریب سایبری

نکات مهم فصل:

- معرفی برخی از پلت فرم ها
- مرور ویژگی های برخی از پلت فرم ها
- مزایا و معایب و کارکرد برخی از پلت فرم ها

سکوی فریب Acalvio ShadowPlex

پیاده‌سازی آن با کنترل مهاجم در مراحل اولیه بهره‌برداری از دارایی‌های کلیدی، امنیت را تقویت می‌کند.
مرکز فریب Acalvio از طریق هوش مصنوعی و تحلیل تهدید، عملکرد آن را بهینه می‌سازد.

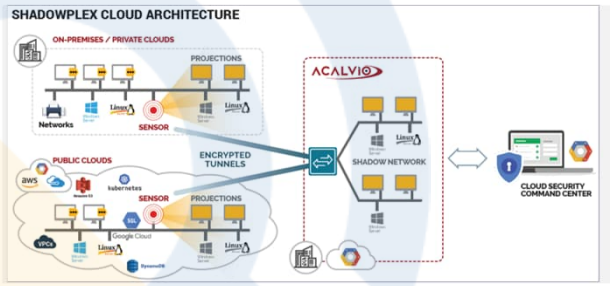
شامل ابزارهایی مانند BOTsink، ThreatStrike و ThreatPath است که به ترتیب برای درگیرسازی، شناسایی مسیرهای حمله و ارزیابی آسیب‌پذیری‌ها طراحی شده‌اند.

قابلیت مسدودسازی و قرنطینه‌سازی حملات را نیز دارد.

به‌منظور شناسایی سریع تهدیدات طراحی شده است تا اقدامات پاسخ پیش از تثبیت مهاجم و استخراج داده‌ها انجام شود.

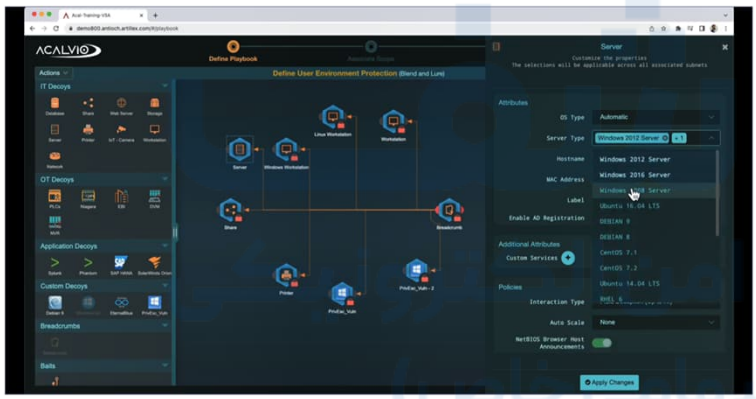
. در مجموع، Attivo با ارائه یک سکو جامع مبتنی بر فریب سایبری، به بهبود شناسایی و مقابله با تهدیدات پیشرفته کمک می‌کند.

معماری Acalvio ShadowPlex



۴۵

افزودن یک کارگزار جدید به یک Playbook در داشبورد مدیریتی Acalvio ShadowPlex



تنوع سرورها

سرورهای مختلف را می‌توان انتخاب کرد.

۴۶

سکوی فریب Acalvio ShadowPlex

ماندگاری

فریب‌های Acalvio ShadowPlex با کوچک‌ترین تلاشی توسط مهاجم در تلاش‌های شناسایی و کشف راه‌اندازی می‌شوند.

افزایش امتیاز

حساب‌های دارای امتیاز جعلی را در اکتیو دایرکتوری به‌عنوان طعمه (هانی توکن‌ها) برای جذب مهاجمی که به دنبال افزایش امتیاز حساب است مستقر می‌کند.

فرار از دفاع

دارای یک موتور مبتنی بر هوش مصنوعی است که پویایی و تازه‌سازی طعمه‌ها را تضمین می‌کند. در نتیجه مهاجم نمی‌تواند از فریب‌ها اثر انگشت بگیرد و احتمال فرار از دفاع را به حداقل می‌رساند.

دسترسی به اعتبارنامه

از طعمه‌ها و هانی توکن‌ها استفاده می‌کند که مهاجمان را جذب می‌کند. هنگامی که این دارایی‌ها با استفاده از اعتبارنامه‌های قانونی مورد دسترسی قرار می‌گیرند، Acalvio ShadowPlex آن اعتبارنامه‌ها را به‌عنوان در معرض خطر شناسایی می‌کند.

کشف

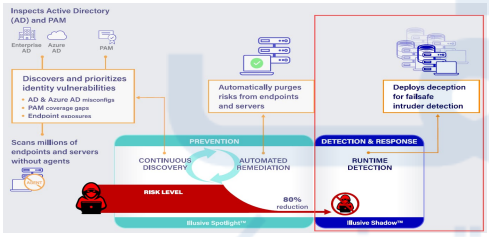
شامل کشف سامانه از راه دور و مبتنی بر شبکه است. اهداف قانونی را مبهم می‌کند و تلاش‌های مهاجمان برای کشف دارایی‌هایی که در معرض خطر قرار می‌گیرند را شناسایی می‌کند.

جمع‌آوری

طعمه‌های Acalvio یا هانی توکن‌ها به‌عنوان اهدافی برای جمع‌آوری مستقر می‌شوند. تلاش برای دسترسی به چنین طعمه‌هایی به عنوان داده ارزشمند ذخیره می‌کند.

معرفی سکوها .....

سکوی فریب Illusive Shadow



سکوی Illusive Shadow بخشی از راه‌حل جامع دفاع سایبری شرکت Illusive است که به شناسایی و پاسخ به تهدیدات مبتنی بر هویت می‌پردازد و از افزایش امتیازات مهاجمان و حرکت جانبی به دارایی‌های حیاتی جلوگیری می‌کند.

حالات کاربرد

این سکوی فریب با استفاده از بیش از 75 تکنیک فعال، فریب‌های باورپذیری را در نقاط پایانی قرار می‌دهد که شبیه داده‌ها و اعتبارنامه‌های واقعی هستند.

پاسخ سریع

با تبدیل هر نقطه پایانی به شبکه‌ای از فریب، شناسایی زودهنگام مهاجمان را تضمین می‌کند و به تیم‌های امنیتی امکان پاسخ سریع به تهدیدات را می‌دهد.

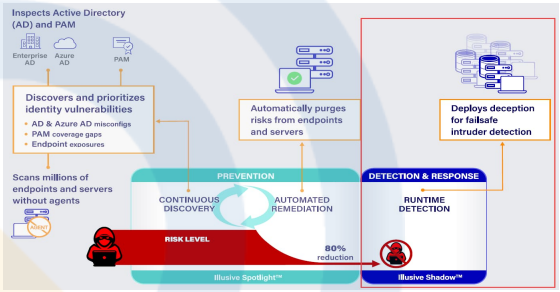
موفق در آزمایش ها

این سکوی فریب به طور مؤثر در بیش از 140 تمرین تیم قرمز با سازمان‌های امنیتی مختلف آزمایش شده و موفق به شناسایی تهدیدات ناشناخته و حفاظت از دارایی‌های کلیدی شده است.

سکوی فریب Illusive Shadow

سکوی Illusive Shadow بخشی از راه‌حل جامع دفاع سایبری شرکت Illusive است که به شناسایی و پاسخ به تهدیدات مبتنی بر هویت می‌پردازد و از افزایش امتیازات مهاجمان و حرکت جانبی به دارایی‌های حیاتی جلوگیری می‌کند.

- بیش از 75 تکنیک فریب، شناسایی و حفاظت بدون عامل فریب خودکار برای هر نقطه پایانی به‌صورت سفارشی
- نمایی از دیدگاه مهاجم از طریق کنسول فایل‌های Beacon فریبنده مایکروسافت آفیس
- به‌گونه‌ای طراحی شده است که تأثیر کمی بر فناوری اطلاعات داشته باشد و از شناسایی شدن توسط مهاجمان جلوگیری کند.
- این سکوی فریب به طور مؤثر در بیش از 140 تمرین تیم قرمز با سازمان‌های امنیتی مختلف آزمایش شده و موفق به شناسایی تهدیدات ناشناخته و حفاظت از دارایی‌های کلیدی شده است.



سکوی Illusive Shadow به‌عنوان بخشی از راه‌حل جامع دفاع سایبری شرکت Illusive

۴۹

پشتیبانی Illusive Shadow از MITRE ATT&CK

- تشخیص فعال‌شدن دسترسی مدیر در یک سامانه
- استفاده از اشتراک‌گذاری‌های شبکه فریبنده،
- نظارت بر تعداد زیادی API Win32 برای مشاهده عملکرد مهاجمان در سطح سیستم‌عامل
- **ارائه قابلیت‌های کامل جرم‌یابی در سطح نقطه پایانی**
- ارائه طیف وسیعی از برنامه‌های کاربردی به‌عنوان ابزارهایی برای کمک به دفاع
- **ایجاد شبکه فریب**
- قراردادن اعتبارنامه‌های فریب بر روی میزبان و ترغیب مهاجم به استفاده از آن‌ها
- **ایجاد کاربران فریب**
- ایجاد ایمیل‌های فریبنده و ایجاد هانی‌توکن‌ها برای فریب مهاجم به سمت سامانه‌های فریب یا خدمات شبکه
- **ایجاد پردازه فریب**

۵۰

معرفی سکوها.....

سکوی فریب CyberTrap

سکوی CyberTrap با هدایت مهاجمان به یک محیط کنترل‌شده، عملیات ردیابی را در داخل شبکه انجام می‌دهد و از آسیب‌رساندن آن‌ها به شبکه جلوگیری می‌کند. این سکوی فریب به‌عنوان لایه اضافی حفاظت در پشت دیواره آتش عمل کرده و از فریب‌های بدون عامل در نقاط کلیدی شبکه استفاده می‌کند.

حالات کاربرد

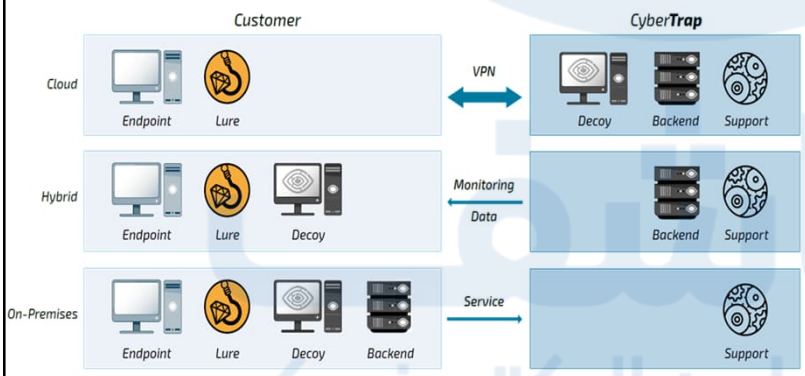
سکوی تله سایبری در سه حالت در محل سازمان، ابری و ترکیبی قابل‌استفاده است و فریب‌های برنامه کاربردی وب و نقطه پایانی را در اختیار دارد.

حمایت از مایتره

به طور مؤثر از چارچوب مایتره پشتیبانی می‌کند و به شناسایی و پاسخ به تهدیدات کمک می‌کند.

۵۱

حالات سکوی فریب CyberTrap



CyberTrap پس از شناسایی مهاجم وی را به یک محیط کنترل‌شده هدایت می‌کند تا عملیات ردیابی را در داخل شبکه به‌منظور جمع‌آوری اطلاعات انجام دهد.

علاوه بر اینکه به مهاجم اجازه گسترش حمله را می‌دهد از آسیب‌رساندن وی به شبکه جلوگیری می‌کند.

۵۲

سکوی فریب CyberTrap

انواع فریب‌ها

فریب
اکتیو
دایرکتوری

هرگونه پویش برای حساب‌های کاربری را شناسایی می‌کند و برای ارسال اعتبارنامه نادرست به مهاجم استفاده می‌کند.

مهاجم به‌طور غیرقابل شناسایی به یک ایمیج فریبنده اکتیو دایرکتوری واقعی در محیط فریب هدایت می‌شود.

مهاجم از این اعتبارنامه‌های نادرست برای حرکت پیشتر در شبکه استفاده کند به دام می‌افتد.

با نظارت دقیق حمله و تحلیل تاکتیک‌های حمله، اکتیو دایرکتوری اصلی نیز در برابر حملات آینده تقویت می‌شود.

۵۳

سکوی فریب CyberTrap - **پشتیبانی از MITRE ATT&CK**

T1190	بهره‌برداری از برنامه‌های کاربردی عمومی	استفاده از فریب برنامه‌های کاربردی وب
T1110	جست‌وجوی فراگیر	استفاده از کارگزارها به‌عنوان فریب با سیستم‌عامل‌ها و برنامه‌های مختلف
T1049	کشف اتصالات شبکه	استفاده از فریب‌ها با خدمات مختلف و طعمه برای جذب مهاجم به تله‌ها
T1021	خدمات راه دور	استفاده از کارگزارهای RDP به‌عنوان فریب و قراردادن فریب‌هایی در شبکه که امکان دسترسی به این کارگزارها را فراهم کنند.
T1039	درایو اشتراکی شبکه	استفاده از فریب‌ها با درایوهای اشتراکی

۵۴

معرفی سکوها.....

سکوی فریب Fidelis

با تحلیل تطبیقی و فناوری فریب هوشمند، آگاهی کامل از موقعیت را ارائه می‌دهد و قوانین درگیری را با تغییر سطح حمله تنظیم می‌کند. این سکوی فریب با استفاده از طعمه‌های معتبر و خرده‌های نان، مهاجمان سایبری و بدافزارها را به لایه فریب کشانده و قبل از آسیب به عملیات سازمانی یا استخراج داده‌ها، آن‌ها را ایزوله می‌کند. از کاربردهای این سکو می‌توان به تشخیص حرکت جانبی، کشف تهدیدات اکتیو دایرکتوری و شناسایی دستگاه‌های اینترنت اشیا آلوده اشاره کرد.

حالات کاربرد

فریب‌ها شامل طعمه‌ها، خرده‌های نان و فریب‌های فعال هستند که به طور مداوم از زمین سایبری نقشه‌برداری کرده و تحلیل مخاطرات را ارائه می‌دهند.

یادگیری ماشین

این سکوی فریب با استفاده از یادگیری ماشین، حرکت جانبی مهاجمان را شناسایی کرده و تاب‌آوری سایبری را بهبود می‌بخشد.

شبیه سازی

همچنین، شبیه‌سازی‌های مخاطرات به بهبود مستمر محل قرارگیری طعمه‌ها و خرده‌های نان کمک می‌کند.

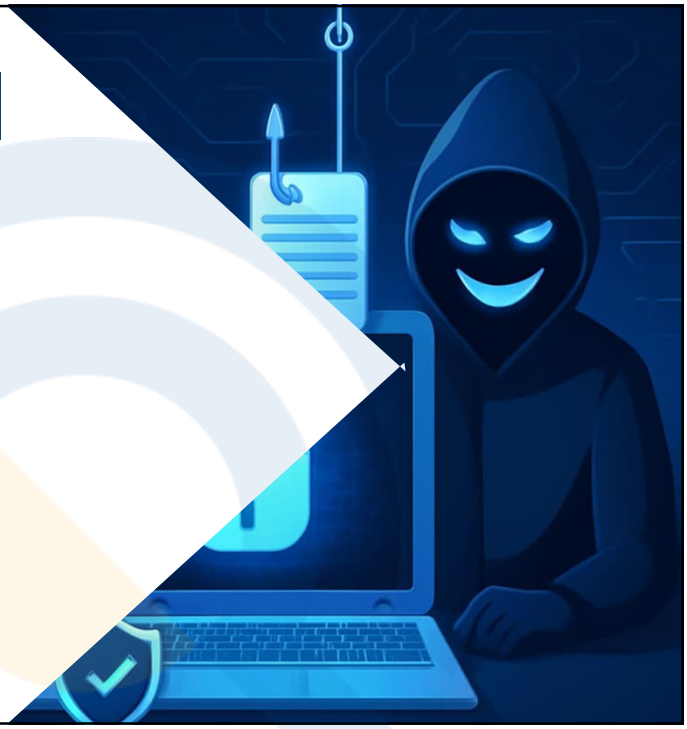
۵۵

مراحل عملکرد Fidelis Deception

مرحله	توضیحات
کشف	نقشه‌برداری دائمی از دارایی‌ها و شبکه ایجاد و به‌روزرسانی دارایی‌ها برای مکان، استفاده و نوع دارایی نتیجه: پایه منحصربه‌فرد ایجادشده برای هر فریب و استقرار
فریب	ساخت لایه فریب از خروجی لایه کشف ایجاد خودکار شبکه فریب مبتنی بر دارایی‌ها، خدمات و پردازه‌های واقعی نتیجه: شبکه فریب واقعی و متقاعدکننده
توزیع	قراردادن خودکار فریب‌ها در شبکه پخش‌کردن خرده‌های نان در دارایی‌های واقعی و اکتیو دایرکتوری نتیجه: توسعه سریع و اثربخشی فوری
شناسایی	هشدارها از دسترسی و درگیری با فریب تحلیل استفاده از داده‌های مسموم نتیجه: تحلیل معتبر داخلی، جعل اعتبارنامه و شناسایی حرکت جانبی
سازگاری	شناسایی دارایی‌های جدید و توپولوژی‌های شبکه به‌روزرسانی خودکار برای نقشه کشف و شبکه فریب نتیجه: دفاع فریب هوشمند و تطبیقی

۵۶

انواع فریب‌ها در سکوی فریب Fidelis



طعمه‌ها

سخت‌افزار: لپ‌تاپ‌ها، کارگزارها، مسیریاب‌ها، سوئیچ‌ها، دوربین‌ها، چاپگرها، دستگاه‌های IoT سازمانی و غیره.
نرم‌افزار: سیستم‌عامل، درگاه‌ها، خدمات، برنامه‌های کاربردی و غیره.
ابر: سیستم‌عامل ابری، برنامه‌های کاربردی ابری و حساب‌های کاربری ابری.

خرده‌های نان

فایل‌ها، سندها، ایمیل‌ها، برنامه‌های کاربردی، اعتبارنامه حافظه، کلیدهای رجیستری، منابع سامانه، فعالیت‌های شبکه، فایل‌های قناری و غیره.
منابع اینترنت اشیا و ابر.

فریب فعال

از یادگیری ماشین برای خودکارسازی و انطباق استفاده از فریب‌ها و خرده‌های نان بر اساس مخاطرات دارایی استفاده می‌کند.
به‌طور فعال حرکت جانبی مهاجم، عملیات انجام‌شده برای شناسایی شبکه و فعالیت‌های وی را تشخیص می‌دهد.

۵۷

معرفی سکوها .....

سکوی فریب TrapX DeceptionGrid

سکوی TrapX DeceptionGrid نرم‌افزاری با فعال‌سازی دفاع پیش‌دستانه، به تیم‌های امنیتی امکان برنامه‌ریزی و استقرار فریب‌ها در برابر سناریوهای حمله مبتنی بر چارچوب مایتره را می‌دهد. با ارائه صدها طعمه معتبر و شبیه‌سازی، این سکو حفاظت جامع و دید مقیاس‌پذیر فراهم می‌کند.

ممیزی نقاط پایانی

قابلیت ممیزی Endpoint وضعیت نقاط پایانی را ارزیابی کرده و هشدارهای دقیق مبتنی بر مایتره را برای تسهیل برنامه‌ریزی دفاع پیش‌دستانه ارائه می‌دهد.

موثر در باج افزار

به طور خاص در شناسایی باج‌افزار، حملات مرد میانی و حرکات جانبی مؤثر است و می‌تواند به‌سرعت حملات را مختل کند.

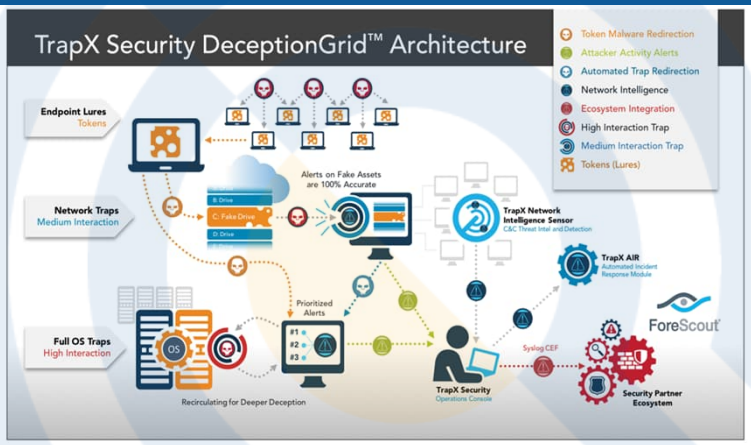
پوشش مناسب مایتره

با قابلیت پوشش نزدیک به 100 فن و راهکنش از مایتره، امکان آزمایش و بهبود مستمر دفاع را فراهم می‌آورد و با ادغام آسان با سایر سامانه‌ها، بهبود تاب‌آوری سایبری و کاهش زمان تشخیص تهدیدات را تضمین می‌کند.

۵۸

سکوی فریب TrapX DeceptionGrid

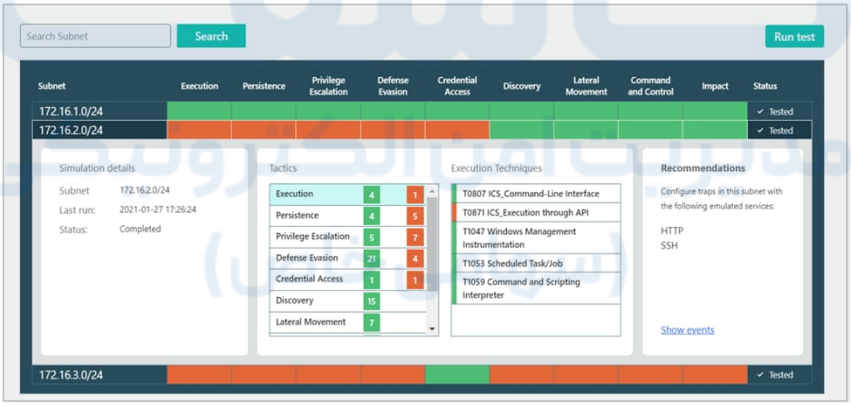
مهم‌ترین مزایای TrapX DeceptionGrid :
محافظت و دید انتها به انتها ،
فریب در عمق: تله‌های بیشتر = مخاطره کمتر ،
ادغام با MITRE ATT&CK



۵۹

سکوی فریب TrapX DeceptionGrid

داشبور مناسب



۶۰

معرفی سکوها.....

سکوی فریب Zscaler Deception

تشخیص تهدید مبتنی بر فریب است که به‌عنوان بخشی از Zscaler Zero Trust Exchange عمل می‌کند و برای شناسایی تهدیدات پیشرفته درون‌شبکه‌ای طراحی شده است. این سکو با استفاده از فریب‌ها و تله‌های عسل، حرکت جانبی مهاجمان، باج‌افزارها و کاربران آسیب‌دیده را شناسایی و متوقف می‌کند.

انحراف از دارایی اصلی

سکوی فریب Zscaler ، فریب‌ها را در محیط عملیاتی قرار می‌دهد تا مهاجمان را از دارایی‌های حیاتی منحرف کند و در مراحل مختلف زنجیره کشتار سایبری، تهدیدات را شناسایی و محدود کند.

ابزار مناسب دفاع

این سکوی فریب به سازمان‌ها کمک می‌کند تا با به‌کارگیری راهبردهای دفاع فعال، به طور مؤثری با حملات مقابله کنند.

۶۱

Zscaler Deception به عنوان بخشی از Zscaler Zero Trust Exchange ارائه شده است

1. **متوقف کردن حرکت جانبی مهاجم** — کارگزارها، برنامه‌های کاربردی و پایگاه‌های داده فریب مستقر در شبکه، مهاجمانی که سعی در حرکت جانبی دارند را شناسایی کرده و آن‌ها را متوقف می‌کنند.
2. **مختل کردن باج‌افزار** — فریب‌هایی که در سراسر محیط قرار می‌گیرند، باج‌افزار را در هر مرحله از زنجیره کشتار شناسایی و محدوده تأثیرگذاری آن را محدود می‌کنند.
3. **شناسایی کاربران در معرض خطر** — از گذرواژه‌ها، کوکی‌ها، نشست‌ها و غیره برای شناسایی کاربران در معرض خطر استفاده می‌کند.
4. **شناسایی استفاده از اعتبارنامه‌های سرقت‌شده** — برنامه‌های وب فریب مهاجمان را با استفاده از اطلاعات کاربری سرقت‌شده برای ورود به سامانه رهگیری می‌کنند.

۶۲

استفاده از فریب در Zscaler Deception
برای برهم‌زدن حملات مراحل مختلف زنجیره کشتار سایبری

تشخیص شناسایی

فریب‌های هوش تهدید فعالیت شناسایی قبل از حمله را تشخیص داده تا اطلاعاتی در مورد حملات خارجی ارائه دهند.

تشخیص بهره‌برداری

فریب‌های ایمیل با مهاجمانی درگیر می‌شوند که تلاش می‌کنند حملات مهندسی اجتماعی/ فیشینگ را بر روی کارکنان با ارزش بالا انجام دهند.

تشخیص دسترسی

اعتبارنامه‌ها، کوکی‌ها و نشست‌های مرورگر به‌عنوان طعمه‌ای عمل می‌کنند تا مهاجمان را فریب داده و آن‌ها را به سمت برنامه‌های فریب هدایت کنند.

تشخیص حرکت جانبی

فریب‌های با ارزش بالا مانند نشست‌های SSH و اشتراک‌گذاری‌های ذخیره‌شده/ درایوهای شبکه نقشه‌برداری‌شده مهاجمانی که به‌صورت جانبی حرکت می‌کنند را رهگیری می‌کنند.

تشخیص ارتقای دسترسی

کاربر و رایانه فریب در اکتیو دایرکتوری، مهاجمانی که در حال شناسایی و خنثی‌سازی هستند را تشخیص داده و افزایش امتیازات را خنثی می‌کنند.

تشخیص سرقت داده

فایل‌های فریب و پردازه‌های فریب در نقاط پایانی، رمزگذاری/ استخراج داده‌ها را تشخیص می‌دهند.

۶۳

مطالعه موردی عملکرد سکوی Zscaler Deception در متوقف‌کردن یک تهدید پیشرفته ناشناخته
در اوایل زنجیره کشتار سایبری در یکی از بزرگترین بانک‌های جهان

نفوذ اولیه — ۱ — در این مرحله مهاجم از طریق یک مسیریاب افشاشده‌ی Wi-Fi سیسکو وارد شبکه می‌شود.

تشخیص اولیه — ۲ — مسیریاب سیسکو یک طعمه Zscaler Deception بوده و بدین‌ترتیب مهاجم شناسایی می‌شود.

گردآوری اطلاعات — ۳ — مهاجم حدود نه ساعت و نیم در شبکه مشغول بوده و به‌صورت مداوم از یک طعمه به طعمه دیگر می‌رود. Zscaler Deception فعالیت مهاجم را ضبط کرده و استراتژی وی را آشکار می‌کند.

بررسی — ۴ — اطلاعات SOC از Zscaler soc SOC اطلاعات Deception را با رویدادها همبسته کرده و متوجه می‌شود مهاجم یک نقطه پایانی را در قسمت دیگری از شبکه در معرض خطر قرار داده است.

دفاع فعال — ۵ — مکان با نقطه پایانی در معرض خطر توسط Zscaler Deception با طعمه‌هایی برای تقویت دفاع محصور شده است.

خنثی‌سازی تهدید — ۶ — نقطه پایانی در معرض خطر از شبکه جدا شده و مهاجم با قطع کانال فرماندهی و کنترل C&C از شبکه بیرون انداخته می‌شود.

۶۴

نسخه‌های Zscaler Deception

قابلیت	مورد استفاده	نسخه استاندارد	نسخه پیشرفته
فریب شبکه	تشخیص حرکت جانبی	کتابخانه فریب کامل	همه موارد موجود در نسخه استاندارد به‌علاوه فریب‌های سفارشی
فریب نقطه پایانی	تشخیص کاربران به‌مخاطره‌افتاده	فریب‌های برنامه کاربردی کوکی‌های مرورگر فایل‌های Beacon	همه موارد موجود در نسخه استاندارد به‌علاوه: تشخیص باج‌افزار تشخیص MITM تشخیص جست‌وجوی فراگیر تشخیص استفاده از اعتبارنامه‌های درون حافظه
فریب اکتیو دایرکتوری	تشخیص حملات به اکتیو دایرکتوری	تشخیص حمله اکتیو دایرکتوری کاربران فریب دامنه‌های متعدد	مشابه نسخه استاندارد
نمای سطح حمله هویت	کشف و اصلاح پیکربندی‌های نادرست خطرناک در اکتیو دایرکتوری	Add-on	مشاهده بی‌درنگ پرخطرترین کاربران / میزبان‌ها شناسایی آسیب‌پذیری‌ها و پیکربندی‌های نادرست به‌محض ظهور استفاده از راهنمایی‌های آماده برای اصلاح و کاهش مخاطرات
ادغام SOC / شکار	هشدار و گردش کار SOC	هشدارهای ایمیل	گردش کار کامل SOC
ویژگی‌های سازمانی	مدیریت حساب کاربری و مدیریت کاربر	Single Sign-On گزارش‌های حسابرسی نقش‌های استاندارد	همه موارد موجود در نسخه استاندارد به‌علاوه: فهرست سفید IP ایستا دسترسی به API

۶۵

معرفی سکوها .....

سکوی فریب Cynet

Cynet 360 یک سکوی تشخیص و پاسخ پیشرفته تهدیدات است که با استفاده از فریب هوشمند و تعامل فریبنده، به شناسایی فعالیت‌های تهدید کمک می‌کند. این سکو از تله‌های عسل برای قراردادن فریب‌ها در محیط استفاده می‌کند و هشدارهایی در مورد حملات شامل باج‌افزار، فایل‌های مشکوک و دسترسی به فریب‌های کاربر تولید می‌کند.

بررسی دسترسی به فایل ها

با تشخیص زمان باز شدن فایل‌های فریب و تلاش‌های غیرمجاز برای دسترسی به منابع، به شناسایی مهاجمان کمک می‌کند.

اطلاعات دقیق

این سکوی فریب با استفاده از داشبوردهای تحلیلی، اطلاعات دقیقی از فعالیت‌های مشکوک ارائه می‌دهد.

۶۶

انواع هشدارها در سکوی فریب Cynet

فایل فریب

این هشدار هنگامی تولید می‌شود که کاربری تلاش می‌کند یکی از فایل‌های فریب ذخیره‌شده روی میزبان‌های محافظت‌شده را باز کند. هشدار شامل نشانی IP میزبانی است که فایل فریب روی آن باز شده است.

کاربر فریب

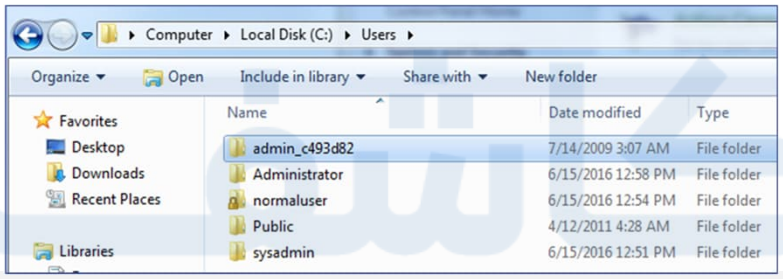
این هشدار هنگامی تولید می‌شود که کاربری تلاش می‌کند با استفاده از یک کاربر فریب به یک میزبان وارد شود.

شبکه فریب

این هشدار هنگامی تولید می‌شود که کاربری تلاش می‌کند به یک میزبان فریب در شبکه دسترسی پیدا کند.

۶۷

نمونه‌هایی از عملیات فریب در سکوی Cynet - آفیس



ایجاد فایل

Cynet سندهای Word، Excel و PowerPoint را در یک مسیر کاربری جدید مانند C:\Users\admin_c493d82 روی میزبان مستقر می‌کند.

نام گذاری

این فایل‌ها دارای نام‌های جذاب برای فریب مهاجمان هستند.

دسترسی دهی

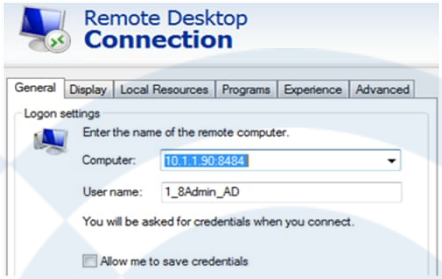
نام حساب کاربری به‌صورت تصادفی ایجاد می‌شود.

بررسی دسترسی ....

برای فایل‌های آفیس فریبنده، Cynet 360 می‌تواند تشخیص دهد که چه زمانی این فایل‌ها در داخل سازمان یا خارج از محیط شبکه محلی سازمان باز می‌شوند.

۶۸

نمونه‌هایی از عملیات فریب در سکوی RDP - Cynet



ایجاد فایل

CYNET یک فایل اتصال RDPذخیره‌شده در همان مسیری که در بالا توضیح داده شد ایجاد می‌کند.

ایجاد اعتبار نامه نامعتبر

فایل اتصال RDPحاوی اعتبارنامه‌های نامعتبر است.

دسترسی دهی

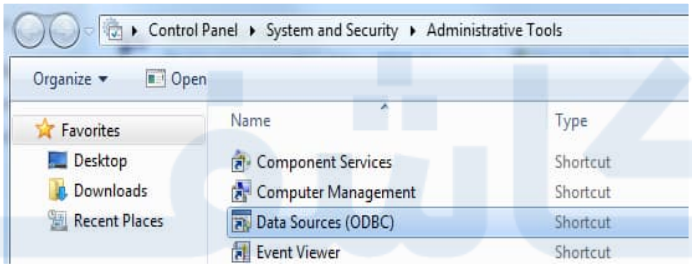
این فایل هنگامی که اجرا می‌شود تلاش می‌کند با اعتبارنامه نامعتبر از طریق درگاه TCP 8484به کارگزار Cynetمتصل شود.

بررسی دسترسی ....

Cynet یک هشدار تولید می‌کند.

۶۹

نمونه‌هایی از عملیات فریب در سکوی ODBC - Cynet



ایجاد فایل

ODBC (Open Database Connectivity)یک API استاندارد باز برای دسترسی به پایگاه‌های داده مانند Access، dBase، DB2وExcelاست.

ایجاد اعتبار نامه نامعتبر

Cynetاز پشتیبانی برنامه‌نویسی داخلی ویندوز برای ODBCبا نصب یک اتصال ODBCبه یک پایگاه داده موجود در محیط استفاده می‌کند.

دسترسی دهی

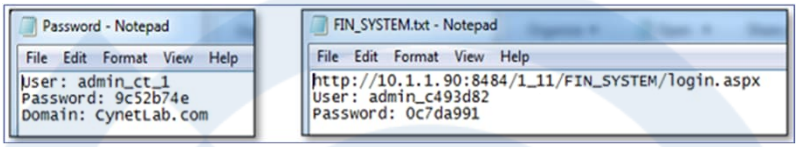
هنگامی که مهاجم تلاش می‌کند از این اتصال ODBCبرای پایگاه داده نامعتبر استفاده کنند .

بررسی دسترسی ....

Cynet یک هشدار تولید می‌کند.

۷۰

نمونه‌هایی از عملیات فریب در سکوی Cynet - فایل تکست



ایجاد فایل

Cynet فایل‌های متنی را با اعتبارنامه نامعتبر در میزبان مستقر می‌کند.

بررسی اعتبار

اگر یکی از این اعتبارنامه‌های نامعتبر استفاده شود.

ایجاد اعتبار نامه نامعتبر

این اعتبارنامه‌ها خود را به‌عنوان اعتبارنامه دامنه یا اعتبارنامه یک برنامه وب داخلی پنهان می‌کنند.

بررسی دسترسی ....

یک هشدار تولید می‌شود.

۷۱

سکوی ماتریس تهدید - ThreatMatrix

محصول ماتریس تهدید خود را به‌عنوان یک سکو مدیریت مستمر تهدیدات معرفی می‌کند که بر شناسایی سریع و دقیق تهدیدات خارجی و داخلی متمرکز است. این سکو با استفاده از فنون فریب سایبری و شبیه‌سازی محیط‌های واقعی، قادر به تشخیص، ردیابی و واکنش به انواع حملات پیشرفته است.

شامل ابزارهایی مانند BOTsink، ThreatStrike و ThreatPath است که به ترتیب برای درگیرسازی، شناسایی مسیرهای حمله و ارزیابی آسیب‌پذیری‌ها طراحی شده‌اند.

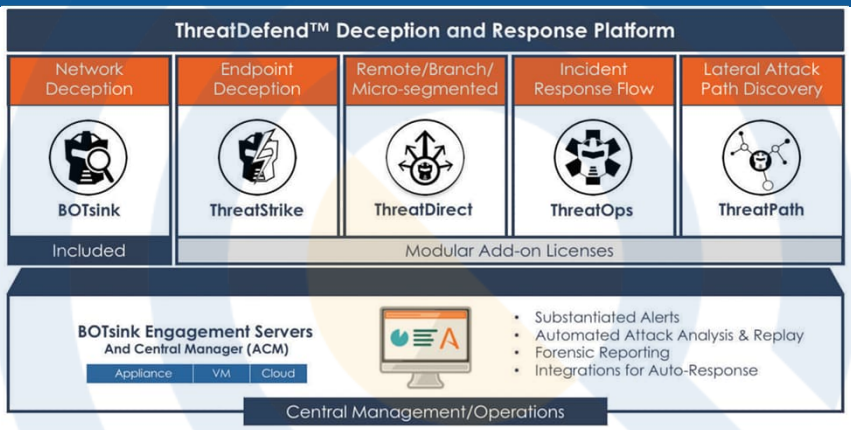
قابلیت مسدودسازی و قرنطینه‌سازی حملات را نیز دارد. در مجموع، Attivo با ارائه یک سکو جامع مبتنی بر فریب سایبری، به بهبود شناسایی و مقابله با تهدیدات پیشرفته کمک می‌کند.

Attivo NETWORKS
ThreatDefend Platform
DECEIVE. DETECT. DEFEND.
www.attivonetworks.com

۷۲

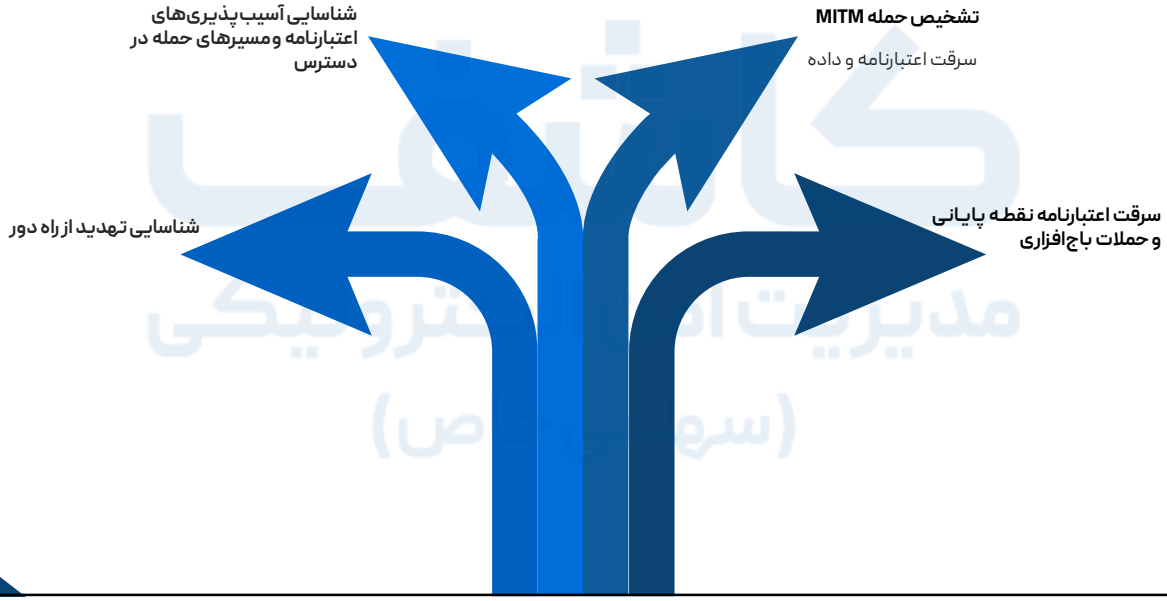
سکوی فریب Attivo ThreatDefend

سکوی فریب و پاسخ Attivo ThreatDefend دسته‌ای از تشخیص تهدید مبتنی بر فریب ایجاد کرده است که از فریب‌های مبتنی بر نقطه پایانی استفاده می‌کند.



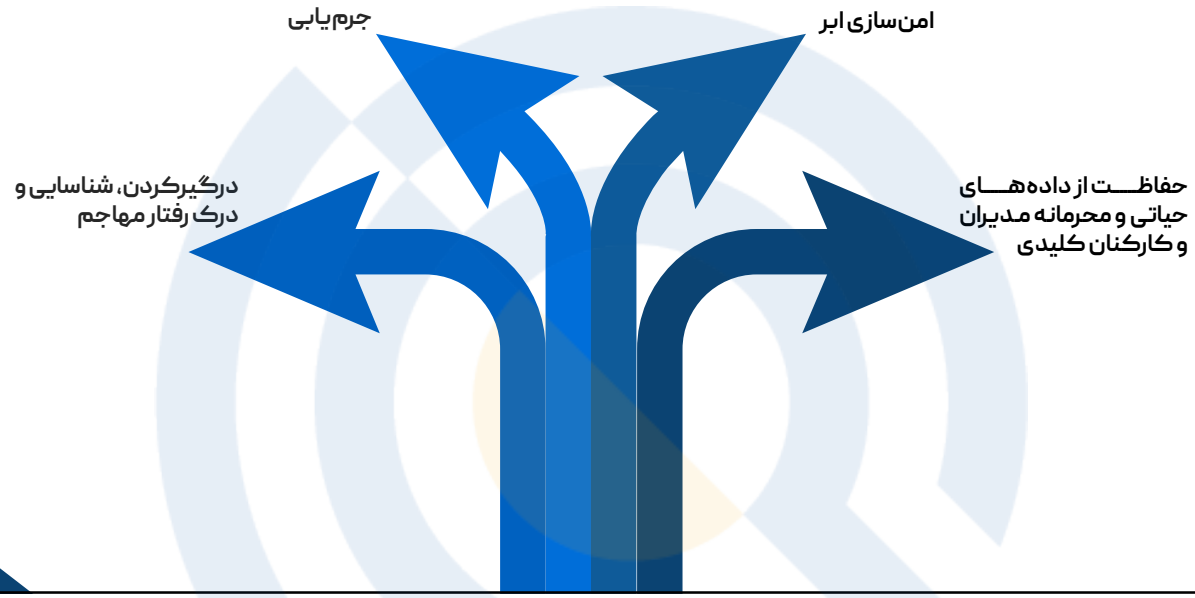
۷۳

مزایا و قابلیت‌ها - سکوی فریب Attivo ThreatDefend



۷۴

مزایا و قابلیت‌ها - سکوی فریب Attivo ThreatDefend



۷۵

فصل ششم

تشریح چند مثال برای کاربری فریب سایبری با استفاده از پلت فرم دیجاوو

نکات مهم فصل:

- سکوی فریب سایبری DejaVu
- تاکتیک دسترسی اولیه - تکنیک Phishing: Spearphishing
- تاکتیک دسترسی به اعتبارنامه - تکنیک جست‌وجوی فراگیر
- تاکتیک دسترسی به اعتبارنامه - تکنیک: MitM مسمومسازی LLMNR/NBT-NS و SMB Relay

DejaVu یک سکوی فریب سایبری منبع باز است که برای استقرار طعمه‌ها در فضای ابری و شبکه داخلی استفاده می‌شود

کارایی دژاوو

هنگامی که مهاجم با طعمه درگیر می‌شود، DejaVu هشدارهایی با دقت بالا تولید می‌کند که باید توسط تیم دفاعی بررسی شوند.

مزایای پیاده‌سازی سناریوهای فریب سایبری با استفاده از **DejaVu**

تشخیص فعالیت‌های مخرب

توانایی تشخیص فعالیت‌های مخرب فراتر از سازوکارهای حفاظتی استاندارد
هشدار زودهنگام بدون تأثیر بر سامانه‌های حیاتی

پیش‌بینی حملات

جمع‌آوری اطلاعات تهدید با نرخ مثبت نادرست پایین در مورد تاکتیک‌های مهاجم
توانایی درک آسان‌تر اهداف، انگیزه‌ها و مقاصد مهاجم

ایجاد اختلال

اثرگذاری در تاکتیک‌ها، تکنیک‌ها و رویه‌های مهاجم

پاسخ‌دهی

دستکاری رفتارها و تعاملاتی که باعث سردرگمی، ایجاد تاخیر یا قطع فعالیت‌های مهاجم می‌شود.
افزایش هزینه مهاجم

۷۸

انواع طعمه در DejaVu

خرده‌نان‌ها
Honey Docs
HoneyHash - Injects creds into memory
Kerberoast Honey Account

کارخواه‌ها ی طعمه
NBNS Decoy
MITM Decoy
SSDP Client
Email Client

کارگزاره ای طعمه
MYSQL
SNMP
TELNET
SMB Server with custom files
FTP
TFTP
Web Server - Tomcat، Apache، Basic Auth
SSH Interactive and Non-Interactive
SMTP
RDP Interactive and Non-Interactive
VNC
HONEYCOMB (To capture events from Honey Docs)
ICS/SCADA Decoys - Modbus and S7COMM

۷۹

مزایا و معایب DejaVu

مزایا

رایگان
سبک
سهولت پیاده‌سازی و کاربرد

معایب

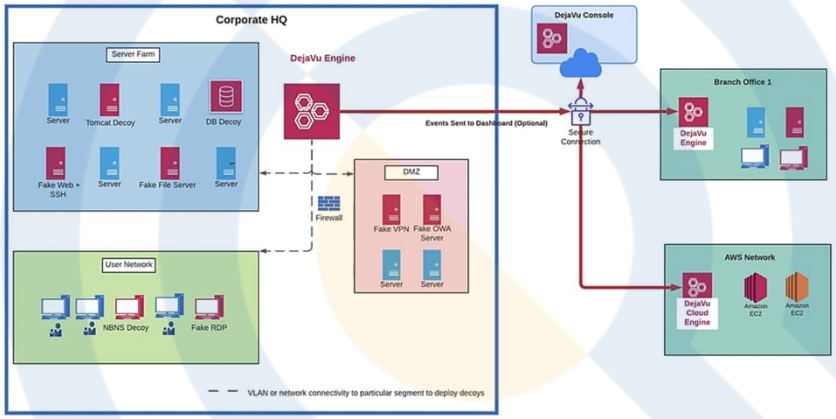
محدودیت پشتیبانی از تاکتیک‌های چارچوب MITRE
نداشتن امکانات کافی برای شخصی‌سازی هشدارها و طعمه‌گذاری

۸۰

معماری DejaVu

این سکو از دو بخش اصلی تشکیل شده است: موتور DejaVu برای استقرار طعمه‌ها در زیرساخت‌های مختلف (دفاتر مرکزی، شعب و ابر) و کنسول DejaVu به‌عنوان داشبورد متمرکز برای مدیریت و مشاهده هشدارها.

طعمه‌ها به سه دسته تقسیم می‌شوند: کارگزارهای طعمه (مانند SSH ،MYSQL ،FTP)، کارخواه‌های طعمه (مانند NBNS، مردمیانی) و خرده‌نان‌ها (مانند Honey Docs ، HoneyHash) این سکو با خودکارسازی فرایند فریب، تشخیص تهدیدات و تحلیل حملات را بهبود می‌بخشد.



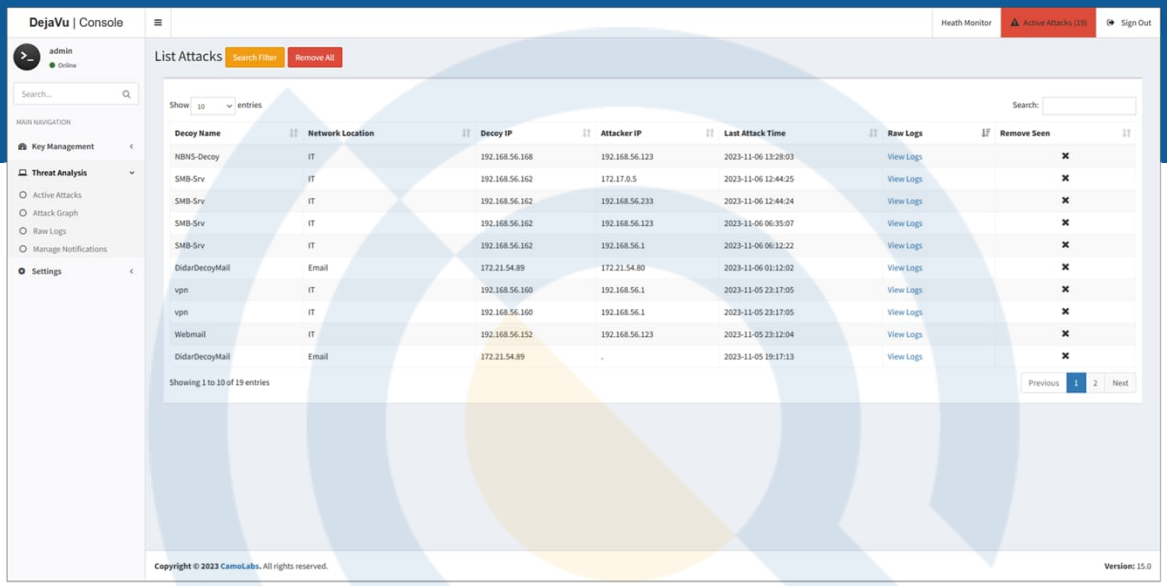
۸۱

موتور DejaVu

با ایجاد حس آشنایی کاذب (دژاوو) در کاربران، رفتار آن‌ها را در محیط‌های مجازی یا سایبری دستکاری می‌کند و به عنوان ابزاری برای فریب و هدایت تصمیم‌گیری‌ها عمل می‌نماید.

۸۲

کنسول DejaVu



۸۳

گراف حمله در کنسول DejaVu

۸۴

مثال هایی از دژاوو

سناریوی اول
فیشینگ هدفمند

اقدامات مهاجم :

تاکتیک دسترسی اولیه

تکنیکPhishing: Spearphishing

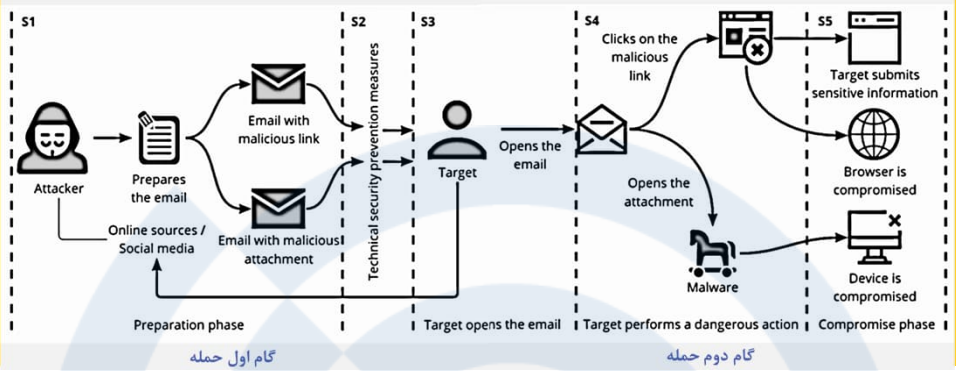
اقدامات دفاعی

ایجاد ایمیل طعمه

۸۵

تاکتیک دسترسی اولیه -
تکنیک Spear phishing:Phishing

۸۶



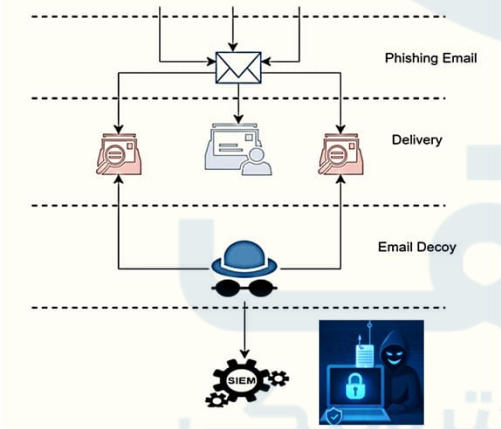
گام‌های حمله Spearphishing

آماده سازی ایمیل

مشخص شدن مخاطب

آلوده سازی

۸۷



طعمه‌گذاری هدفمند

نمای دریافت ایمیل توسط DejaVu

گام1
ایجاد ایمیل طعمه برای کاربر جعلی

گام2
ایجاد حساب کاربری در شبکه‌های اجتماعی

گام3
ایجاد کارخواه ایمیل طعمه در DejaVu و پایش آن

مثال هایی از دژاوو

سناریوی دوم
جمع آوری اطلاعات

اقدامات مهاجم

تاکتیک شناسایی : تکنیک جمع‌آوری اطلاعات شبکه قربانی

تاکتیک دسترسی به اعتبارنامه : تکنیک حمله جست‌وجوی فراگیر

اقدامات دفاعی

ایجاد طعمه برای خدمت ایمیل و خدمت VPN

۸۹

تاکتیک شناسایی -
تکنیک جمع‌آوری اطلاعات شبکه قربانی

۹۰

گام شناسایی زیردامنه‌ها

استفاده از ابزار Sublist3r

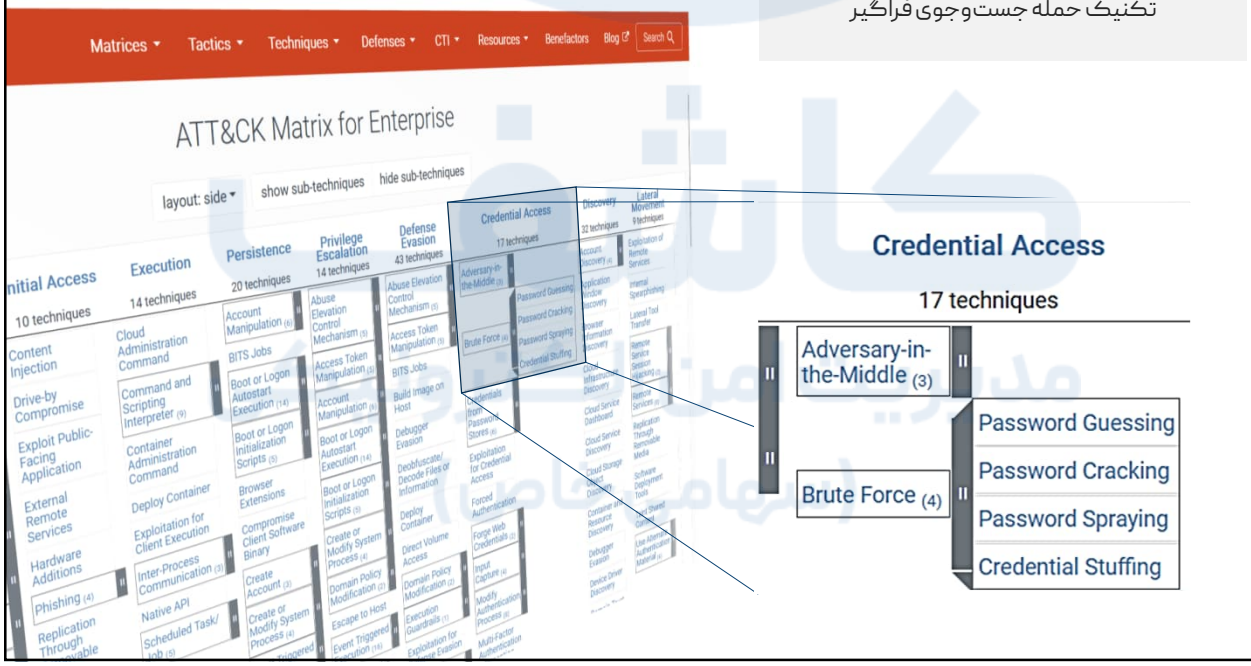
Sublist3r یک ابزار متن‌باز پایتون برای شناسایی زیردامنه‌های یک دامنه با استفاده از OSINT است. از موتورهای جستجو و منابع مانند Google، Bing، VirusTotal و DNSdumpster برای جمع‌آوری اطلاعات استفاده می‌کند. این ابزار برای تست نفوذ قانونی و شناسایی نقاط ضعف کاربرد دارد، اما استفاده غیرمجاز آن غیرقانونی است.

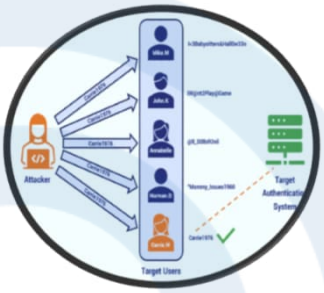
Sublist3rابزاری برای شناسایی زیردامنه‌ها در تست نفوذ است که با OSINT و bruteforce سطح حمله را نقشه‌برداری می‌کند.

```
┌──(root㉿kali)-[/home/kali]
└─# sublist3r -d modares.ac.ir

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for modares.ac.ir
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[!] Error: Google probably now is blocking our requests
[-] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 56
www.modares.ac.ir
acda.modares.ac.ir
afre.modares.ac.ir
aijh.modares.ac.ir
bb.modares.ac.ir
```

۹۱

اقدامات ثانویه -
تکنیک حمله جست‌وجوی فراگیر





حمله اسپری گذرواژه

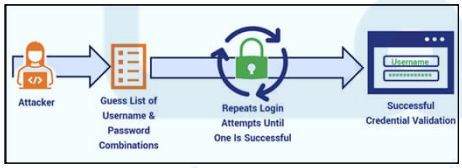
حمله اسپری گذرواژه تکنیکی است که در آن هکر از یک رمز عبور رایج برای تعداد زیادی حساب کاربری یا نام کاربری در یک سیستم یا چندین سیستم استفاده می‌کند تا قفل حساب‌ها را دور بزند و دسترسی غیرمجاز به دست آورد.

حمله واژه‌نامه

حمله واژه‌نامه با استفاده از لیست کلمات رایج برای حدس زدن رمز عبور به منظور دسترسی غیرمجاز انجام می‌شود.

حمله جست‌وجوی فراگیر ترکیبی

حمله جست‌وجوی فراگیر ترکیبی با ترکیب دیکشنری و brute-force، رمزهای عبور را با تولید تغییرات هدفمند کلمات رایج می‌شکند.

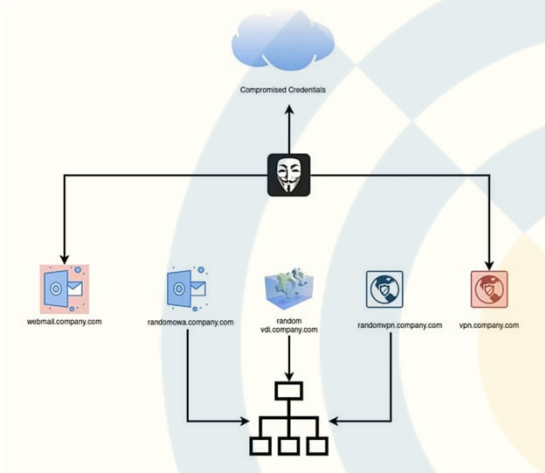


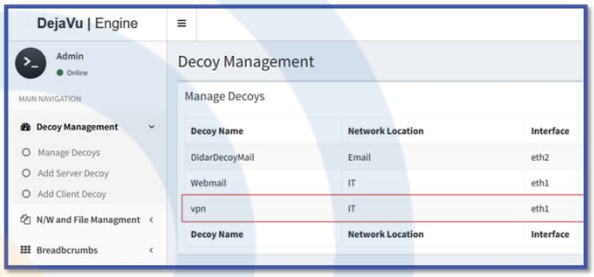
حمله جست‌وجوی فراگیر ساده

حمله جست‌وجوی فراگیرروشی است که در آن تمام ترکیب‌های ممکن کاراکترها (حروف، اعداد، نمادها) به‌صورت سیستماتیک و متوالی برای شکستن رمز عبور یا کلید رمزنگاری آزمایش می‌شوند، بدون استفاده از الگوهای خاص یا لیست کلمات.

اقدامات دفاعی

توسط DejaVu - ایجاد طعمه برای خدمت ایمیل و خدمت VPN





۹۵

مثال هایی از دژاوو

سناریوی سوم
مسموم سازی

اقدامات مهاجم

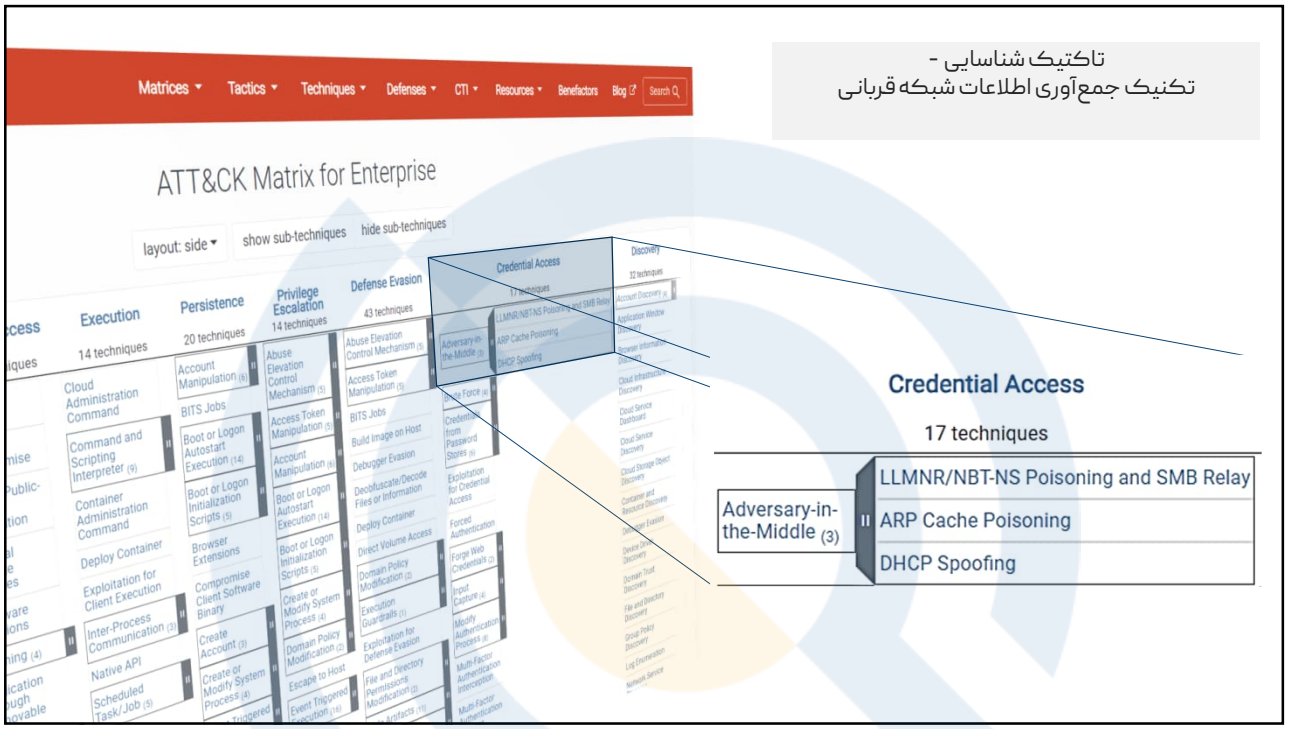
تاکتیک دسترسی به اعتبارنامه
MitM:
تکنیک:
مسموم‌سازی LLMNR/NBT-NS و
SMB Relay

اقدامات دفاعی

ایجاد طعمه برای خدمت ایمیل و
خدمت VPN

۹۶

تاکتیک شناسایی -
تکنیک جمع‌آوری اطلاعات شبکه قربانی



بررسی برخی از مفاهیم در این تکنیک

LLMNR
(Link-Local Multicast Name Resolution):

پروتکلی در ویندوز که در شبکه‌های محلی، در صورت عدم پاسخگویی DNS، از طریق ارسال درخواست‌های چندپخشی، نام‌های شبکه‌ای (مانند نام هاست‌ها) را به آدرس IP تبدیل می‌کند و در صورت مسمومسازی، اعتبارنامه‌ها را در معرض سرقت قرار می‌دهد.

NBT-NS
(NetBIOS Name Service):

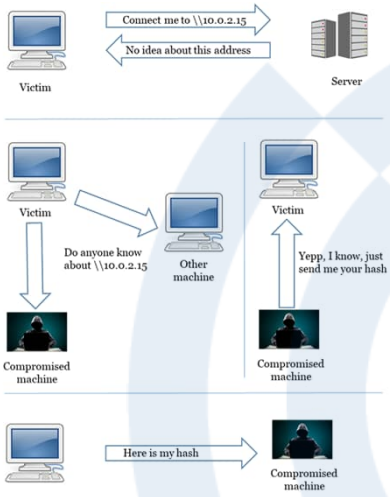
پروتکلی برای تبدیل نام‌های NetBIOS به آدرس IP در شبکه‌های محلی که با پخش درخواست‌ها عمل می‌کند و در صورت مسمومسازی، امکان سرقت هش‌های NTLM را فراهم می‌سازد.

SMB
(Server Message Block)

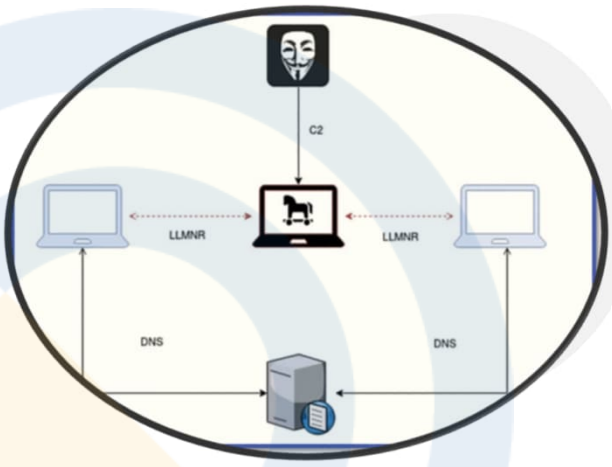
پروتکلی برای اشتراک‌گذاری فایل، چاپگر و ارتباطات بین سیستم‌ها در شبکه که در حمله SMB Relay، اعتبارنامه‌های سرقت‌شده برای دسترسی غیرمجاز به منابع شبکه‌ای استفاده می‌شوند.

۹۸

روش های مسموم سازی



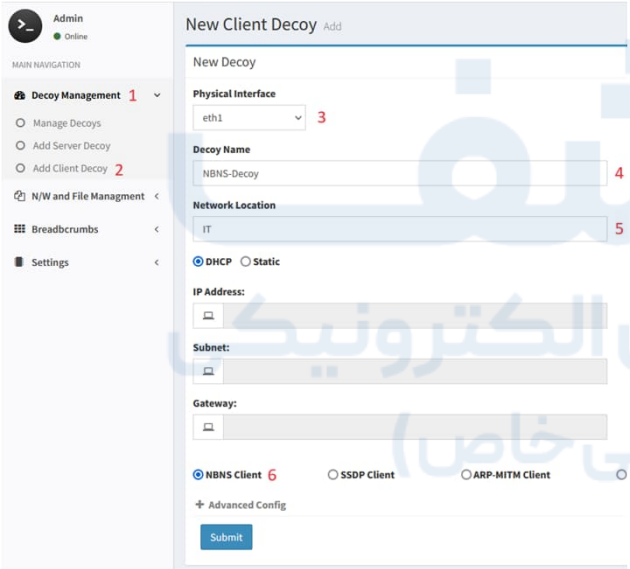
نحوه مسموم سازی

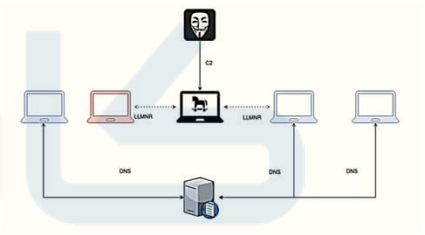


نحوه قرارگیری مهاجم در شبکه

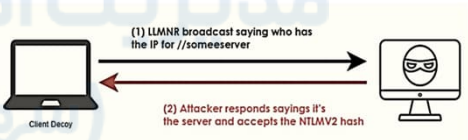
۹۹

ایجاد خدمت NBNS طعمه در DejaVu





نمای قرارگیری کارخواه طعمه در شبکه



پس از ایجاد کارخواه طعمه مهاجم به محض پاسخ دهی شناسایی می‌شود.

۱۰۰