خبرنامه الکترونیکی ۶۰

مرکز تخصصی آپا دانشگاه سمنان

شماره ششم، سال ششم، خرداد ۱۴۰۲ | کاری از تیم تولید محتوای مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

داکر چیست؟

https://cert.semnan.ac.ir info.cert@semnan.ac.ir 023-31535019 @semcert

هـــر تمـــاس و پیامـــی از طـرف هـر موسسـه‌ای کـه شـــما را پـــای خودپـــرداز بکشـــاند حتما **کلاهبرداری** است.

فهرست

خبر

آموزش

مرکز آپا دانشگاه سمنان

خبر

آگاهی از امنیت سایبری کارکنان در استراتژی‌های دفاعی در مرکز توجه قرار می‌گیرد!

به گفته Fortinet، با تشدید حملات سایبری، سازمان‌های بیشتری نیاز به داشتن یک فرهنگ امنیتی قوی برای همه کارکنان را تشخیص می‌دهند.

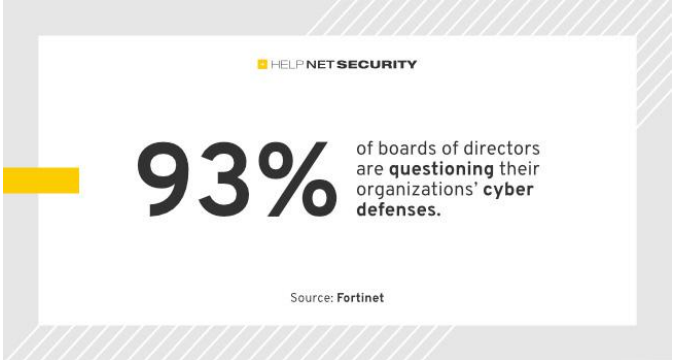
آگاهی کارکنان از امنیت سایبری

جدیدترین گزارش از آزمایشگاه FortiGuard شرکت Forti-net نشان می‌دهد که تهدیدات باج افزاری در اوج خود باقی می‌مانند و هیچ مدرکی دال بر کند شدن آن در سطح جهانی وجود ندارد. همچنین، Fortinet دریافت که 84٪ از سازمان‌ها یک یا چند رخنه را در سال 2022 تجربه کردند.

آخرین تحقیقات Fortinet نشان می‌دهد که بیش از 90 درصد از رهبران بر این باورند که افزایش آگاهی از امنیت سایبری کارکنان به کاهش وقوع حملات سایبری کمک می‌کند. ازآنجایی‌که سازمان‌ها با خطرات سایبری فزاینده ای روبرو هستند، این تحقیق نقش مهم کارکنان را در خدمت به‌عنوان اولین خط دفاعی سازمان در محافظت از سازمان خود در برابر جرائم سایبری برجسته می‌کند.

فقدان دانش امنیت سایبری در بین کارکنان

81 درصد از سازمان ها در سال گذشته با حملات بدافزار، فیشینگ و رمز عبور مواجه شدند که عمدتاً کاربران را هدف قرار داده بودند. این نشان می‌دهد که کارکنان می‌توانند ضعیف‌ترین نقطه سازمان یا یکی از قوی‌ترین دفاع‌های آن باشند.85 درصد از رهبران می‌گویند که سازمان آنها یک برنامه آموزشی و آگاهی امنیتی دارد، با این حال بیش از 50 درصد معتقدند که کارکنان آنها هنوز دانش امنیت سایبری ندارند. این شکاف نشان می‌دهد که برنامه‌های آموزشی موجود ممکن است به اندازه‌ای که می‌توانست مؤثر نباشند، در نتیجه ناهماهنگی در نحوه اعمال شیوه‌های بهداشت سایبری خوب توسط کارکنان یا اینکه آموزش به اندازه کافی تقویت نشده است.



متمرکز بودن هیئت مدیره بر امنیت سایبری

از آنجایی که بسیاری از حملات کاربران را هدف قرار می‌دهند، به نظر می‌رسد که هیئت مدیره می‌بینند - یا به زودی خواهند دید - که آگاهی از امنیت سایبری کارکنان بخش مهمی از «معادله دفاعی» است. 93 درصد از سازمان‌ها اظهار داشتند که هیئت مدیره آنها در مورد استراتژی و دفاع سایبری سازمان ها سؤال می‌کنند.

جان مدیسون، EVP محصولات و CMO در Fortinet گفت: «خلاصه تحقیقات جهانی ما در مورد آگاهی و آموزش امنیتی 2023 بر نقش حیاتی کارکنان در جلوگیری از حملات سایبری تأکید می‌کند. این نیاز حیاتی سازمان‌ها را برای اولویت‌بندی خدمات آموزشی و آگاهی امنیتی برای اطمینان از اینکه کارکنان به عنوان اولین خط دفاعی خدمت می‌کنند، برجسته می‌کند».

با یک برنامه آموزشی قوی، سازمان‌ها می‌توانند آگاهی کارکنان در مورد ریسک سایبری را بالا ببرند و آنها را برای دفاع از سازمان توانمند سازند و پایه‌ای برای فرهنگ امنیت سایبری قوی و آماده ایجاد کنند. سازمان‌ها می‌دانند که به راه‌حل‌های پیشرفته امنیت سایبری نیاز دارند و گواهی‌های فناوری، قابلیت‌های امنیت سایبری تیم‌های فناوری اطلاعات آنها را ایجاد می‌کنند. تا به امروز، آگاهی کارکنان ممکن است آنطور که باید مورد توجه قرار نگرفته باشد، با این حال می تواند در مبارزه با حملات سایبری در سال های آینده نقشی اساسی داشته باشد.

آسیب‌پذیری پلاگین وردپرس «Gravity Forms» در برابر تزریق شی PHP

افزونه وردپرس «Gravity Forms» در برابر تزریق شی PHP

یک آسیب‌پذیری امنیتی جدید با شناسه CVE-2023-28782 و امتیاز ۸.۳ در افزونه پریمیوم وردپرس «Gravity Forms» کشف شده است. درحال حاضر بیش از ۹۳۰۰۰ وب‌سایت از خدمات افزونه وردپرس استفاده می‌کند و این آسیب‌پذیری ساختار امنیت افزونه و یکپارچگی وب‌سایت‌ها را تهدید می‌کند. آسیب‌پذیری CVE-2023-28782 در برابر تزریق شیء PHP آسیب‌پذیر است. این آسیب‌پذیری خطر قابل توجهی را برای کاربران ایجاد می‌کند.

Gravity Forms یک فرم سفارشی است که صاحبان وب‌سایت‌ها برای ایجاد صفحه پرداخت، ثبت نام، آپلود فایل یا هر فرم دیگری استفاده می‌کنند. این فرم‌ها برای تعاملات یا تراکنش‌های بین بازدیدکننده و سایت مورد نیاز است. Gravity Forms در وب‌سایت خود ادعا می‌کند که توسط طیف گسترده‌ای از شرکت‌های بزرگ از جمله PennState، NASA، Nike، ESPN، Airbnb و Unicef استفاده می‌شود. این آسیب‌پذیری همه افزونه‌ها را از نسخه‌ی 2.7.3 و پایین‌تر تحت تأثیر قرار می‌دهد. این نقص توسط PatchStack در ۲۷ مارس ۲۰۲۳ کشف شد و توسط فروشنده با انتشار نسخه 2.7.4 رفع شد که این نسخه در ۱۱ آوریل ۲۰۲۳ در دسترس قرار گرفت. به مدیران وب‌سایت‌هایی که از Gravity Forms استفاده می‌کنند توصیه می‌شود که در اسرع وقت به‌روزرسانی امنیتی موجود را اعمال کنند.

جزئیات نقص

علت اصلی این آسیب‌پذیری، تابع maybe_unserialize است. که از عدم بررسی ورودی ارائه شده توسط کاربر برای تابع 'maybe_unserialize' ناشی می‌شود و می‌تواند با ارسال داده‌ها به فرم ایجاد شده با Gravity Forms فعال شود. PatchStack در گزارش‌اش هشدار می‌دهد: "از آنجایی که PHP امکان سریال سازی اشیاء را فراهم می‌کند، یک کاربر احراز هویت نشده می‌تواند رشته‌های سریال شده ad-hoc را به یک تماس غیرسریالی آسیب‌پذیر ارسال کند و در نتیجه یک شیء(های) PHP دلخواه به محدوده برنامه تزریق شود." توجه داشته باشید که این آسیب‌پذیری می‌تواند در نصب یا پیکربندی پیش‌فرض افزونه Gravity Forms فعال شود. هر کاربر احراز هویت نشده می‌تواند با ارسال به یک فیلد فهرست در فرمی که با استفاده از Gravity Forms ایجاد شده است، تزریق شی PHP را راه‌اندازی کند.

در کل، پیامدهای آسیب‌پذیری CVE-2023-28782، با توجه به عدم وجود زنجیره POP[1] قابل توجه در پلاگین آسیب‌پذیر در زمان این افشاگری، به‌طور قابل‌توجهی محدود است. با این حال، زمانی که یک افزونه یا تم اضافی یک زنجیره POP را در سایت وردپرس معرفی می‌کند، خطر تشدید می‌شود. این setup نامطمئن به طور بالقوه مهاجم را با توانایی حذف فایل‌های دلخواه، تهیه داده‌های حساس یا اجرای کد بسته به زنجیره POP موجود، مسلح می‌کند. خوشبختانه، اقدامات سریعی برای کاهش این آسیب‌پذیری فاجعه بار انجام شده است. در Gravity Forms نسخه ۲/۷/٤ به این موضوع پرداخته شده و این نقص را برطرف کرده‌اند. همچنین مهم است که به‌روزرسانی‌ها را در همه افزونه‌های فعال در سایت وردپرس خود اعمال کنید، زیرا رفع آسیب‌های امنیتی ممکن است بردارهای حمله مانند زنجیره‌های POP را که می‌توانند در این مورد برای راه‌اندازی حملات آسیب‌رسان مورد استفاده قرار گیرند، حذف کنند.

includes/fields/class-gf-field-list.php, function get_field_input

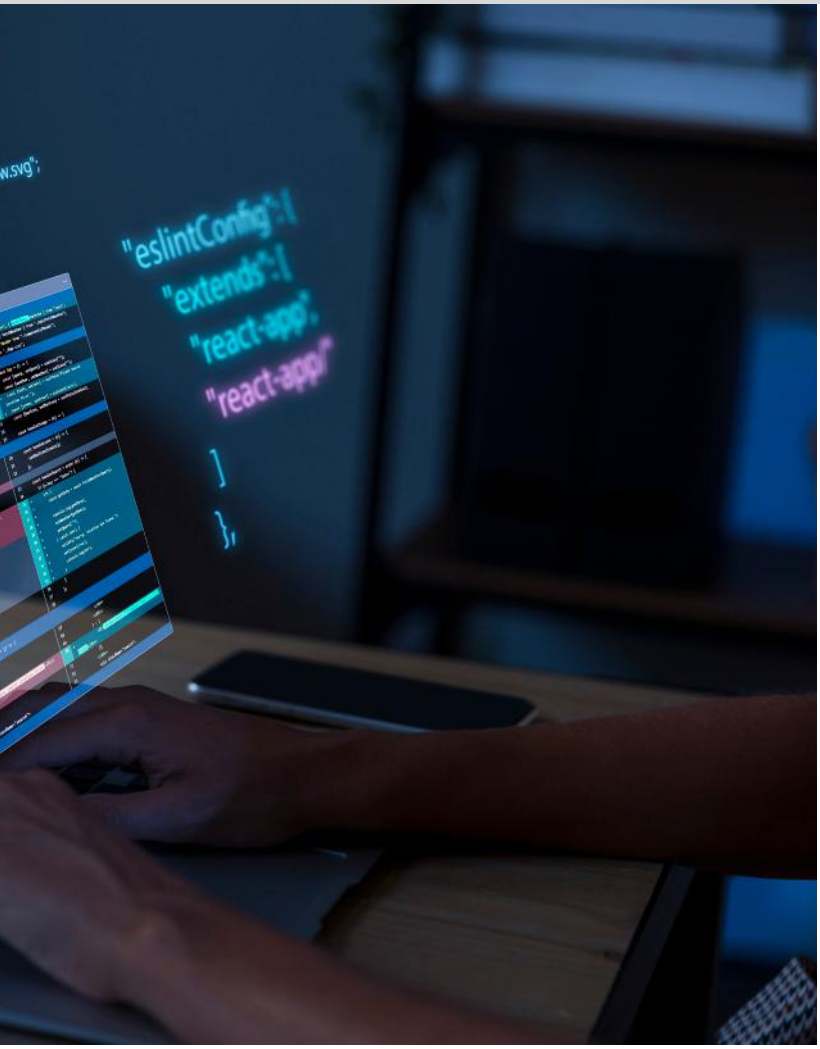
```
public function get_field_input( $form, $value = '', $entry = null ) {

    if( GF_Common::is_legacy_markup_enabled( $form ) ) {
        return $this->get_legacy_field_input( $form, $value, $entry );
    }

    $form_id         = $form['id'];
    $is_form_editor = $this->is_form_editor();

    if ( ! empty( $value ) ) {
        $value = maybe_unserialize( $value );
    }
```

1-property-oriented programming

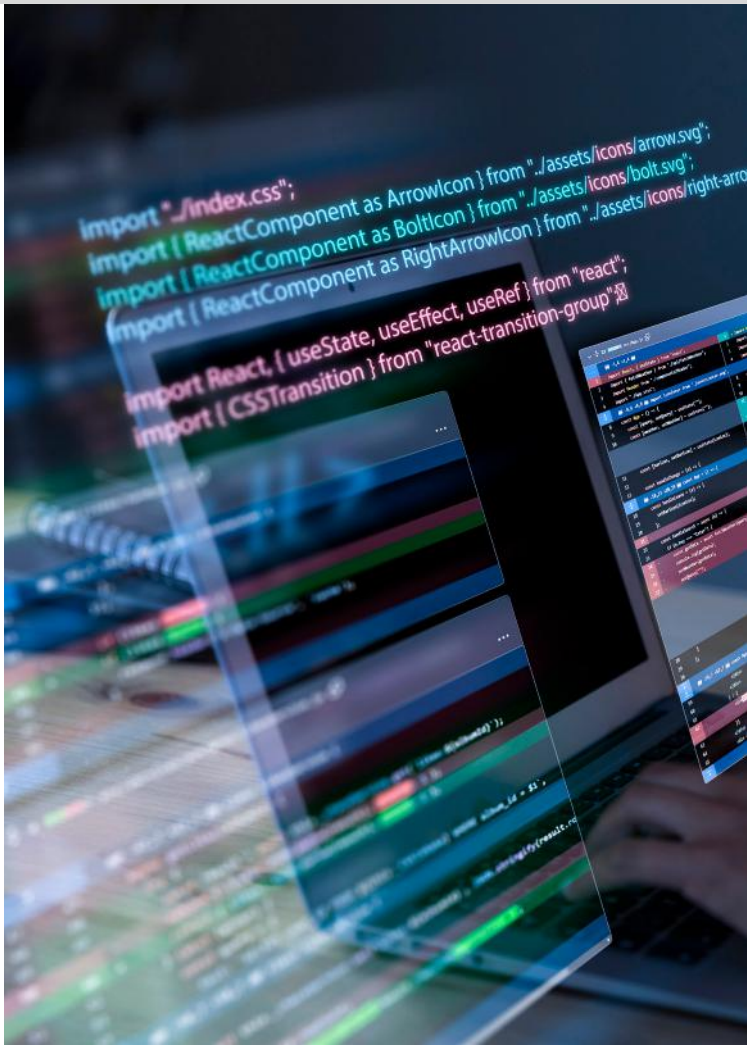


بدافزار اندرویدی iRecorder در گوگل پلی

محققان ESET، یک تروجان دسترسی از راه دور[1] جدید را در فروشگاه Google Play پیدا کردند که در یک برنامه ضبط صفحه نمایش اندروید پنهان شده بود. این برنامه ده‌ها هزار بار نصب شده بود. برنامه «iRecorder - Screen Recorder»، درحالی‌که برای اولین بار در سال 2021 به فروشگاه اضافه شد، از طریق یک به‌روزرسانی مخرب که تقریباً یک سال بعد منتشر شد، به تروجان آلوده شد. نام‌گذاری این برنامه، درخواست مجوز برای ضبط صدا و دسترسی به فایل‌ها را در دستگاه‌های آلوده آسان‌تر می‌نمود زیرا طبیعتا از یک ابزار ضبط صفحه نمایش انتظار می‌رود که چنین مجوزهایی را درخواست نماید. این برنامه قبل از حذف، در فروشگاه Google Play بیش از 50000 بار نصب شده بود و کاربران را در معرض آلودگی‌های بدافزاری قرار داد. استفانکو یکی از محققان ESET گفت: «به دنبال اطلاع‌رسانی ما در مورد رفتار مخرب iRecorder، تیم امنیتی Google Play آن‌را از فروشگاه حذف کرد. با این حال، توجه به این نکته که این برنامه را همچنان می‌توان در مارکت‌های جایگزین و غیررسمی اندروید یافت نیز حائز اهمیت است. توسعه‌دهنده iRecorder برنامه‌های دیگری را نیز در Google Play ارائه می‌کند، اما آن‌ها حاوی کد مخرب نیستند.

بدافزار مورد بحث که AhRat نام‌گذاری شده است، مبتنی بر یک تروجان دسترسی از راه دور اندرویدی منبع‌باز معروف به نام AhMyth است. این تروجان دارای طیف گسترده‌ای از قابلیت‌ها، از جمله ردیابی مکان دستگاه‌های آلوده، سرقت گزارش‌های تماس، مخاطبین و پیام‌های متنی، ارسال پیام‌های کوتاه، گرفتن عکس و ضبط صدای پس‌زمینه است. اما به همین قابلیت‌ها محدود نمی‌شود. پس از بررسی دقیق‌تر، ESET دریافت که برنامه مخرب ضبط صفحه نمایش، تنها از زیرمجموعه‌ای از قابلیت‌های RAT استفاده می‌کند، زیرا فقط برای ایجاد و استخراج صداهای ضبط شده

1-RAT



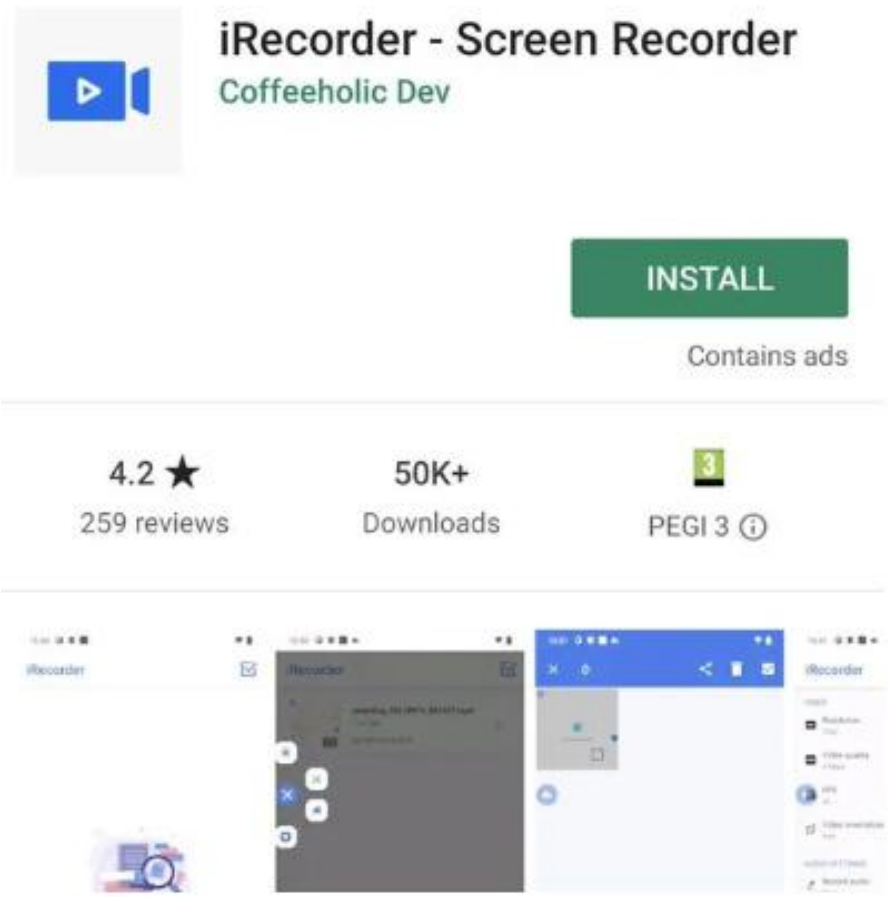
Tribe، که با نام APT۳۶ نیز شناخته می‌شد، مورد استفاده قرار می‌گرفت.

APT۳۶ یک گروه جاسوسی سایبری است که به دلیل استفاده گسترده از تکنیک‌های مهندسی اجتماعی و هدف قرار دادن سازمان‌های دولتی و نظامی در جنوب آسیا شناخته شده است. با این وجود، ما نمی‌توانیم نمونه‌های فعلی را به هیچ گروه خاصی نسبت دهیم.

به روز رسانی: یکی از سخنگویان گوگل پس از انتشار مقاله، بیانیه زیر را به اشتراک گذاشت: وقتی برنامه‌هایی را که خط‌مشی‌های ما را نقض می‌کنند، می‌یابیم اقدامات لازم را انجام می‌دهیم. کاربران همچنین توسط Google Play Protect محافظت می‌شوند. Google Play Protect می‌تواند به کاربران در مورد برنامه‌های مخرب شناسایی شده در دستگاه‌های اندرویدی هشدار دهد.

محیطی و سرقت فایل‌هایی با پسوندهای خاص کاربرد دارد که به فعالیت‌های جاسوسی احتمالی اشاره می‌کند.

این اولین نمونه از نفوذ بدافزار اندروید مبتنی بر AhMyth به فروشگاه Google Play نیست. ESET جزئیاتی درباره برنامه دیگری که در سال ۲۰۱۹ توسط AhMyth به تروجان آلوده شده بود را منتشر کرد. این برنامه با ظاهر شدن در قالب یک برنامه پخش رادیویی، فرآیند بررسی اپلیکیشن گوگل را دو بار فریب داد. استفانکو گفت: « AhMyth پیش از این توسط Transparent



سوء استفاده از کانال‌های جدید برای حملات فیشینگ

سوء استفاده از کانال‌های جدید برای حملات فیشینگ

تیم Perception Point افزایش ۳۵۶ درصدی را در تعداد حملات فیشینگ پیشرفته‌ای که توسط عوامل تهدید در سال ۲۰۲۲ انجام شده است شناسایی کرده‌اند. به طور کلی، تعداد کل حملات ۸۷ درصد افزایش یافته است که نشان‌دهنده تهدید رو به رشدی است که حملات سایبری اکنون برای سازمان‌ها ایجاد می کنند.

افزایش یافتن حملات فیشینگ

در طول سال ۲۰۲۲، تیم Perception Point چندین روند نگران کننده را تجزیه و تحلیل کرد. اولاً، عوامل مخرب همچنان به ابزارهای جدید و پیشرفت‌های هوش مصنوعی[1] و یادگیری ماشین[2] دسترسی گسترده‌ای دارند که فرآیند ایجاد حملات را ساده و خودکار می‌کند.

در نتیجه، آن‌ها به طور فزاینده‌ای قادرهستند بدون زحمت حملات پیچیده‌ای را انجام دهند. مشخصه بسیاری از آنها مهندسی اجتماعی و همچنین تکنیک‌های فرار از جمله تغییر مسیر URL است که شناسایی آن‌ها را به عنوان مخرب برای قربانی دشوار می‌کند. این تیم همچنین شناسایی کرد که چگونه چشم‌انداز تهدید به دلیل به کارگیری سریع برنامه‌های جدید همکاری ابری، فضای ذخیره‌سازی ابری و خدمات برای بهره‌وری و همکاری خارجی تغییر می‌کند.

عوامل تهدید ابزارهای حمله خود را متمرکز کرده‌اند و فراتر از ایمیل و مرورگرهای وب به این برنامه‌ها و خدمات رسیده‌اند. در حالی که ایمیل و مرورگر همچنان بردارهای اصلی حمله باقی مانده‌اند، درسال ۲۰۲۲ شاهد افزایش ۱۶۱ درصدی حملات در سایر کانال‌ها بودیم.

ثابت شد که فیشینگ فراگیرترین تهدید است و ۶۷/۴ درصد از کل حملات را به خود اختصاص داده است. در سال ۲۰۲۲ شاهد افزایش قابل توجه حملات ایمیل تجاری[3] بودیم که ۸۳ درصد رشد کرد. حملات BEC، که در آن مجرمان سایبری جعل هویت کسب وکارهای قانونی و استفاده از تکنیک‌های مهندسی اجتماعی و همچنین[4] برای به دست آوردن مبالغ هنگفت پول یا داده‌های محرمانه هستند، اغلب شناسایی برای راه‌حل‌های امنیتی سنتی ایمیل دشوار است.

ضعیف ترین لینک

علاوه بر این، این نوع حملات که مبتنی بر متن هستند، کارکنان فردی را که ضعیف‌ترین حلقه در زنجیره امنیتی یک سازمان هستند، هدف قرار می‌دهند، حتی زمانی که بسیار آموزش دیده باشند.

یورام سالینجر، مدیر عامل Perception Point، گفت:

«درحالی‌که چشم‌انداز تهدید جهانی به تکامل خود ادامه می‌دهد، ما داده‌های حیاتی را به اشتراک می‌گذاریم که افزایش شهاب سنگی درتعداد حملات را به همراه تکنیک‌های حمله پیچیده تر که برای نفوذ و آسیب رساندن به سازمان‌ها طراحی‌شده‌اند، به تصویر می‌کشد.»

این گزارش نیاز سازمان‌ها را برای محافظت از افراد خود در برابر تهدیدات مدرن در کانال‌های متعدد تجاری و همکاری را روشن میکند. این محافظت میتواند با تقویت یا جایگزینی سیستم‌های امنیتی سنتی با خدمات پیشگیری موثر و خدمات اصلاحی سریع در صورت لزوم، انجام شود.

1-AI
2-ML
3-BEC
4-thread hijacking

چک لیست سیاست های رمز عبور در اکتیو دایرکتوری

مرکز آپا دانشگاه سمنان

آیا تنظیمات مربوط به Store passwords using reversible encryption انجام شده است؟

مطمئن شوید که Disabled باشد

آیا تنظیمات مربوط به Enforce password history تنظیم شده است؟

تنظیم برای بالای 24 پسورد

آیا تنظیمات مربوط به Account lockout duration' is set to انجام شده است؟

مقدارش 15 دقیقه یا بیشتر باشد

آیا تنظیمات مربوط به Maximum password age تنظیم شده است؟

حداکثر 60 روز یا کمتر

آیا تنظیمات مربوط به Account lockout threshold انجام شده است؟

تلاش برای ورود نامعتبر 10 بار یا کمتر باشد

آیا تنظیمات مربوط به Minimum password age تنظیم شده است؟

تنظیم برای یک روز یا بیشتر

آیا تنظیمات مربوط به Reset account lockout counter after انجام شده است؟

مقدارش 15 دقیقه یا بیشتر باشد

آیا تنظیمات مربوط به Minimum password length انجام شده است؟

تعداد کاراکتر 14 یا بیشتر

آیا تنظیمات مربوط به Password must meet complexity requirements فعال گردیده است؟

مطمئن شوید که Enabled باشد

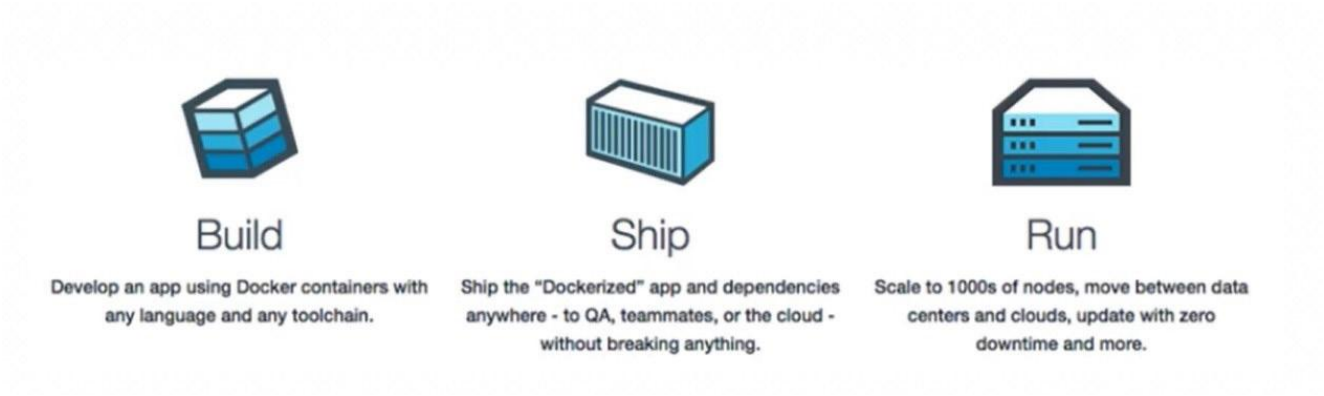
ارائه شده توسط مرکز تخصصی آپا دانشگاه سمنان

مرکز آپا دانشگاه سمنان

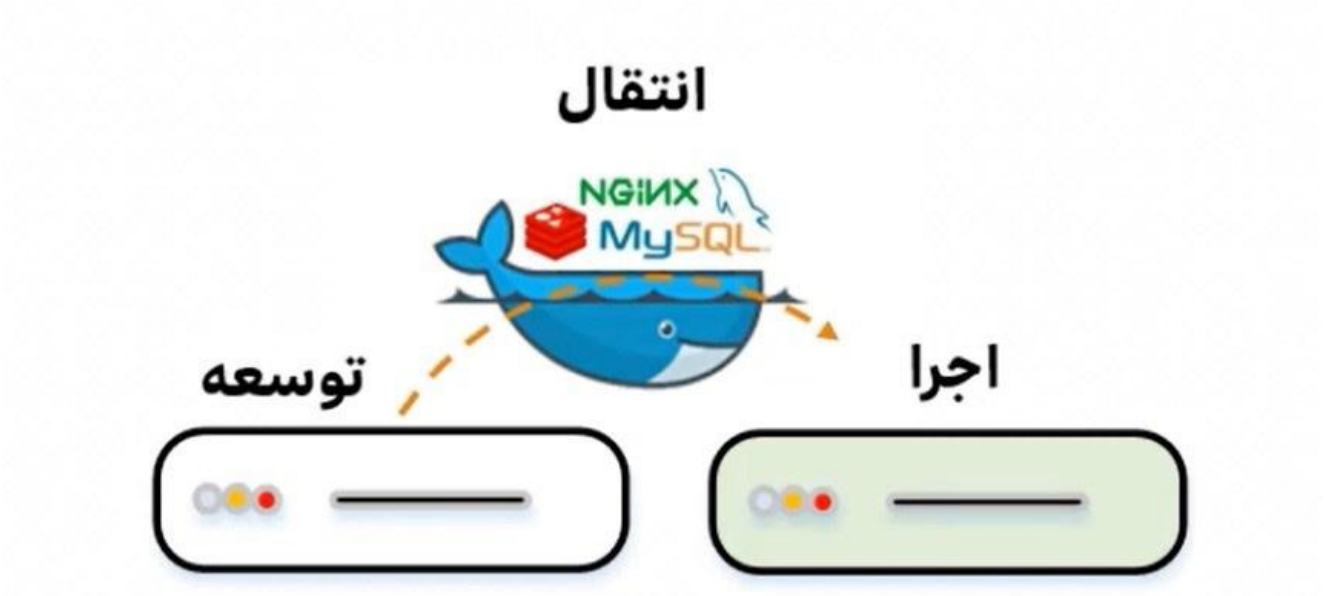
آموزش

داکر

داکر یک platform متن باز است که برای توسعه دادن[1]، انتقال دادن[2] و اجرا[3] استفاده می‌شود.



یکی از بزرگترین مزایای داکر این است که این قابلیت را به توسعه‌دهندگان می‌دهد که برنامه نویسان به طور کامل برنامه‌ها را از کتابخانه‌ها و باینری فایل‌های سیستمی که بر روی آن، برنامه را اجرا کردند مجزا کنند و در واقع همین ویژگی است که فرایند توسعه، انتقال و ساخت را به سریع‌ترین شکل ممکن فراهم می‌کند. این که برنامه از سیستم‌عامل یا زیرساخت مستقل باشه این مزیت را دارد که اگر ما بخواهیم برنامه را در سیستم‌عامل دیگر اجرا کنیم اگر داکر را نصب کنیم می‌توانیم خیلی راحت و سریع پیاده‌سازی را انجام دهیم. مثلا اگر ما برنامه را روی لینوکس توسعه داده‌ایم و حال قصد داریم برنامه را در ویندوز سرور اجرا کنیم اگر داکر وجود نداشت، باید برنامه را روی سرور مقصد از اول می‌نوشتیم در صورتی که با استفاده از داکر خیلی راحت این انتقال را انجام می‌دهیم.



1-Develop
2-Shipping
3-Running

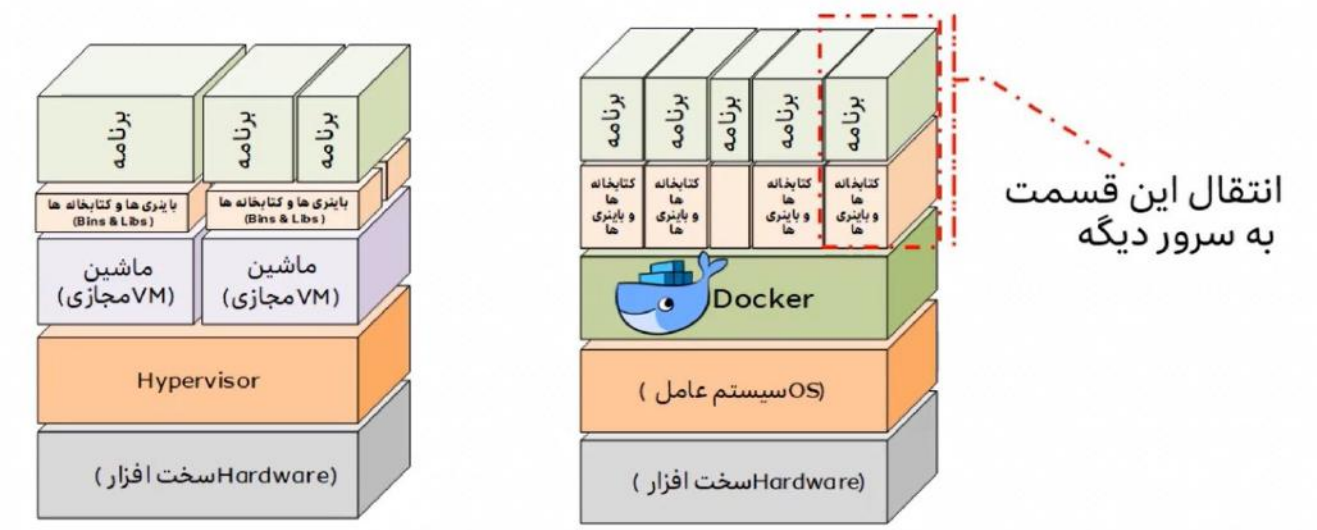
داکر در سال ۲۰۱۳ توسط شرکت ارائه‌دهنده خدمات هاستینگ بوجود آمده است. در حال حاضر شرکت‌های آمازون و گوگل خدمات مبتی بر داکر به مشتری ارائه می‌دهند و شرکت‌های معروفی در حوزه آی تی در زیرساخت خود از داکر استفاده می‌کنند. چون داکر این قابلیت را می‌دهند که در سرور برنامه‌های بیشتری را اجرا کنند، که هم باعث می‌شود هزینه تجهیزات پایین آیند و هم مصرف انرژی. همچنین خیلی راحت‌تر برنامه‌ها را مدیریت می‌کنند. مثلا در آپدیت کردن، جابه‌جایی سرور و گسترش دادن سرویس‌های شرکت‌ها.

مقایسه Docker و ماشین مجازی[1]

داکر این قابلیت را به ما می‌دهد که برنامه‌ها را روی یک محیطی به اسم Container اجرا کنیم، Containerها روی کرنل سیستم‌عامل به صورت مستقیم اجرا می‌شوند و به صورت یک پروسس هستند بر خلاف ماشین‌های مجازی.

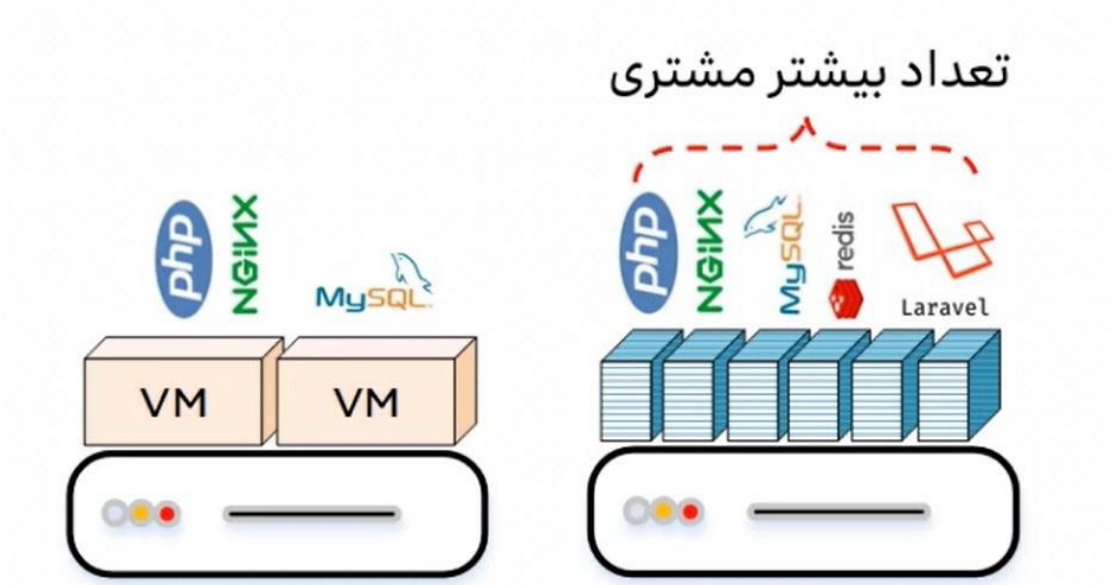
اگر با ماشین‌های مجازی کار کرده باشیم می‌دانیم اگر بخواهیم روی سیستمی ماشین مجازی را اجرا کنیم باید یک هایپروایزر[2] روی آن سخت افزار داشته باشیم که بتوانیم فضای ثابتی از رم، هارد و CPU را به آن اختصاص دهیم از طرفی این واسط مجازی‌ساز سرعت عملکرد را به شدت کند می‌کند و حتی اگر VM ما از همه آن رم و CPU و هاردی که به آن اختصاص داده‌ایم استفاده نکند. ما نمی‌توانیم این منابع را به ماشین مجازی دیگری اختصاص دهیم. در هر ماشین مجازی ما کتابخانه‌ها و باینری فایل‌های خاص خودش را داریم که برنامه‌ها به طور مستقیم بر روی این کتابخانه‌ها و باینری فایل‌ها اجرا می‌شود.

در مقابل ماشین مجازی ما مفهوم Container را داریم که داکر معروف‌ترین پلتفرم هاست. در ساختار Container بر روی سیستم‌عامل، پلتفرم داکر قرار می‌گیرد. این پلتفرم برنامه‌ها را با کتابخانه‌ها و باینری فایل‌های مخصوص خودشون اجرا می‌کنند و اگر ما بخواهیم برنامه را به سرور دیگری منتقل کنیم می‌توان برنامه و باینری فایل‌های آن را برداریم و بر روی سرور دیگری قرار دهیم.



با کمک Container ما می‌توانیم تعداد بیشتری از برنامه‌ها را مستقل از سرور و برنامه‌های دیگر اجرا کنیم. این برای شرکت‌هایی که اسکیل بزرگی دارند خیلی مفید است مثلا به جای اینکه روی سرور ۱۰ تا ماشین مجازی بسازد تا به مشتری خدمات بدهد با استفاده از Container می‌توانند روی سرور به ۱۰۰ کاربرد خدمت بدهد که خب از لحاظ تجهیزات بسیار به صرفه‌تر است.

1-VM
2-Hypervisor



همچنین در صورتی که شرکت‌ها با کمبود تجهیزات سخت‌افزار مواجه شوند (مثلا تعداد کاربران خیلی زیاد می‌شود و لود سیستم بالا رود.) در این حالت شرکت‌ها می‌توانند Containerها را به سرور دیگر منتقل کنند تا لود سیستم کاهش بیابد.

چرا برای توسعه‌دهندگان و سیستم ادمین‌ها استفاده از داکر مزیت دارد؟

توسعه‌دهندگان و سیستم ادمین‌ها زمان خود را صرف نگهداری از سیستم[1] یا رفع باگ‌های سیستم، Scale کردن سیستم (افزایش CPU RAM و ...)، گرفتن Backup و آپدیت کردن سیستم بدون down - time می‌کنند که این کارها زمان بر بوده و یا منجر به قطع شدن سیستم برای مدتی می‌شود . همچنین وقتی دو سرویس متفاوت داریم که با ورژن‌های مختلف برنامه یا زبان برنامه‌نویسی کار می‌کنند مدیریت آن برای توسعه‌دهنده و سیستم ادمین سخت است در صورتی که با Container کردن اپلیکیشن‌ها خیلی راحت و مستقل از هم دیگر، سرویس‌ها اجرا می‌شود یا به عبارتی با استفاده از داکر Conflict version بوجود نمی‌آید.

در کل داکر بسیار سریع هست و سبب بهبود چرخه توسعه اپلیکیشن می‌شود. داکر این امکان را به ما می‌دهد چرخه CICD[2] رابه خوبی اجرا کنیم. به این خاطر که Container محیطی را فراهم می‌کند که اگر روی سیستم توسعه دهنده اپلیکیشن را توسعه دهیم و سپس روی محیط عملیاتی[3] اپلیکیشن را انتقال بدهیم و می‌توانیم برنامه را به راحتی اجرا کنیم به عنوان مثال توسعه‌دهنده باگی را روی سرویس تشخیص می‌دهد همچنین از آن سرویس، همزمان چند صد کاربر استفاده می‌کنند توسعه دهنده می‌تواند مشکل برنامه را در محیط دولوپ یا سرور تست حل کند و بعد از رفع مشکل آن را به Production Server منتقل کرده و آنجا از آن Container اجرا کند و این یعنی کمترین زمان ممکن برای قطع شدن سرور.

داکر از نظر بستر پیاده‌سازی منعطف است و سریع و Portable اجرا می‌شود چون داکر برنامه‌ها را تحت محیط Container فراهم می‌کند و باعث می‌شود که ما بتوانیم روی سرور لینوکس یا ویندوز، دیتا سنتر یا سرورهای Cloud provider برنامه‌ها را اجرا کنیم. حتی به دلیل سرعت بالا و حجم کم Containerها، می‌توان صورت داینامیک تعداد Containerها را در سرویس کم یا زیاد کنیم.

داکر بر خلاف ماشین‌های مجازی از هایپروایزر استفاده نمی‌کند و این باعث شده که حجم کم و سرعت بالایی داشته باشد بنابراین از منابع سیستم استفاده بهینه می‌کند مثلا برای ارائه وب سرویس نسبت به ماشین‌های مجازی، سخت افزار کمتری را نیاز دارد این یعنی هزینه کمتر هم برای خدمات دهنده و هم برای مشتری نهایی.

1-Maintenance
2-Continuous deployment Continuous Integration
3-Production Server

تلاش ما
حفظ امنیت
شماست...