شرکت آب منطقه‌ای گلستان

نشریه داخلی شرکت آب منطقه‌ای گلستان/ شماره دوم / اردیبهشت ماه ۱۴۰۴

دنیای بدافزارها، تعریف و شناسایی

MALWARE

KEVIN MITNICK

زباله می‌تواند جزئیات مهمی را برای
هکرها ارائه دهد: نام، شماره تلفن،
اصطلاحات داخلی یک شرکت

نشریه داخلی شرکت آب منطقه‌ای گلستان

شماره دوم ـــ اردیبهشت ماه ۱۴۰۴

فهرست

دکتر امیرحسین رحیمیان

دنیای بدافزارها، تعریف و شناسایی

در دنیـای امروز، اسـتفاده روزمره از اینترنـت و ابزارهای دیجیتـال اجتناب‌ناپذیر شـده، اما همراه با ایـن راحتی، تهدیداتی هم به وجـود آمده‌اند که امنیت اطلاعات کاربران را به خطـر می‌اندازند. بدافزارها (Malware) یکی از رایج‌ترین و خطرناک‌ترین ابزارهای هکرها برای نفوذ، سرقت اطلاعات، و خرابکاری دیجیتال هستند. شناخت این تهدیدات، نخستین گام برای محافظت در برابر آن‌هاست.

بدافـزار (مخفـف «Malicious Software») به هرگونه برنامه، کد یا فایل مخربی گفته می‌شـود که به‌منظور آسـیب رسـاندن، سـرقت اطلاعات یا کنترل غیرمجاز از سیستم‌ها طراحی شـده است. بدافزارها می‌تواننـد به‌صورت مخفی وارد سیسـتم کاربر شـوند، خود را تکثیر کنند، یا داده‌هـا را رمزگذاری کرده و باج‌گیری کنند.

انواع مهم بدافزارها

01
ویروس (Virus)
ویروس‌ها فایل‌های دیگر را آلوده می‌کنند و با باز شـدن آن‌ها فعال می‌شـوند. ممکن اسـت فایل‌ها را حذف یا تغییر دهند و به‌سرعت در سیستم‌های متصل پخش شوند.

02
کرم (Worm)
کرم‌ها بدون نیاز به فایل میزبان تکثیر می‌شـوند و می‌توانند به‌صورت خودکار از طریق شـبکه گسترش پیدا کنند. از معروف‌ترین آن‌ها می‌توان به ILOVEYOU اشاره کرد.

03
تروجان (Trojan Horse)
ظاهر بی‌خطر دارند (مثل نرم‌افزارهای مفید) اما پس از اجرا دسترسـی مخفی به سیسـتم ایجاد می‌کنند. درب پشتی برای هکر باز می‌شود.

04
روت‌کیت (Rootkit)
به هکر اجازه می‌دهد تا کنترل سطح پایین سیستم را به‌دست بگیرد. معمولاً شناسایی و حذف آن بسیار سخت است و در عمق سیستم پنهان می‌شود.

05 **باج‌افزار (Ransomware)**

فایل‌های قربانی را رمزگذاری می‌کند و برای بازگرداندن دسترسی، درخواست باج می‌دهد. باج‌افزارها تهدید شماره یک کسب‌وکارها هستند(مثلاً WannaCry).

06 **جاسوس‌افزار (Spyware)**

اطلاعات شخصی، رمزهای عبور، یا فعالیت‌های کاربر را مخفیانه جمع‌آوری می‌کند. معمولاً بدون اطلاع کاربر نصب می‌شود.

07 **کی‌لاگر (Keylogger)**

کی‌لاگرها تمامی دکمه‌های زده‌شده روی کیبورد را ذخیره می‌کنند و برای هکر ارسال می‌کنند. هدف اصلی آن‌ها سرقت رمز عبور و اطلاعات ورود است.

08 **تبلغات ناخواسته (Adware)**

تبلیغات مزاحم را روی سیستم نمایش می‌دهد و گاهی حتی اطلاعات مرور کاربر را نیز جمع‌آوری می‌کند. برخی از آن‌ها به بدافزار تبدیل می‌شوند.

شیوه‌های توزیع بدافزار

بدافزارها از مسیرهای مختلفی وارد سیستم می‌شوند:

- ایمیل‌های فیشینگ با پیوست آلوده
- دانلود فایل از سایت‌های نامعتبر
- فلش USB یا هارد اکسترنال آلوده
- شبکه‌های ناامن یا وای‌فای عمومی
- نصب نرم‌افزارهای کرک‌شده و جعلی
- به‌روزرسانی‌های تقلبی یا جعلی مرورگرها

08 **روش‌های شناسایی بدافزار**

۱. نشانه‌های رفتاری در سیستم:

- کند شدن ناگهانی سیستم
- باز شدن صفحات تبلیغاتی غیرعادی
- نصب شدن نرم‌افزارهایی بدون اطلاع
- از کار افتادن آنتی‌ویروس یا فایروال
- ارسال خودکار ایمیل از حساب کاربر

09

۲. استفاده از ابزارها و سرویس‌ها:

- اسکن با آنتی‌ویروس معتبر (Kaspersky, Bitdefender, ESET)
- استفاده از ابزارهای تخصصی مانند Malwarebytes یا ESET Online Scanner
- بررسی فعالیت‌های غیرمعمول در Task Manager و Startup

۳. بررسی آنلاین فایل‌ها:

10

- استفاده از سرویس‌هایی مانند VirusTotal.com برای تحلیل فایل‌ها و لینک‌های مشکوک

جمع‌بندی نهایی

بدافزارها متنوع، پیچیده و در حال تکامل هستند. اما با شناخت درست، رعایت نکات بهداشتی دیجیتال، استفاده از ابزارهای امنیتی، و پرهیز از رفتارهای پرخطر، می‌توان تا حد زیادی از نفوذ آن‌ها جلوگیری کرد.

به خاطر داشته باشید:

امنیت دیجیتال، با آگاهی آغاز می‌شود.

A PRACTICAL GUIDE

••• راهنمای عملی

چگونه از ورود ویروس و بدافزار به سیستم خود جلوگیری کنیم؟

در دنیای پرسرعت دیجیتال امروز، شما شاید با تنها یک کلیک، همه‌چیز را از دست بدهید: اطلاعات شخصی، اسناد کاری، عکس‌های خانوادگی، یا حتی دارایی‌های مالی‌تان. اما خبر خوب این است که بیشتر تهدیدات سایبری - به‌ویژه ورود بدافزار - با چند اقدام ساده ولی مداوم قابل پیشـگیری‌اند. در این بخش، ما با نگاهی عمیق و کاربردی به ۱۰ راهکار عملی می‌پردازیم که مثل واکسن، از شما در برابر آلودگی سایبری محافظت می‌کنند.

01

همیشه آنتی‌ویروس به‌روز داشته باشید
دفاع اول، همیشه فعال

یک آنتی‌ویروس خوب مثل یک نگهبان دائم‌الخدمت است که جلوی در خانه دیجیتال شما ایستاده. اما این نگهبان باید آموزش‌دیده، به‌روز، و آماده مقابله با تهدیدات جدید باشد.

چرا آنتی‌ویروس کافی نیست اگر به‌روز نباشد؟

بدافزارها به‌صورت روزانه تولید می‌شوند – هزاران نمونه جدید در هر ساعت. یک آنتی‌ویروس قدیمی نمی‌تواند آن‌ها را شناسایی کند. آپدیت روزانه یعنی «شناخت تهدیدات جدید.»

نکات کاربردی:

- به‌روزرسانی خودکار را فعال کنید و هفته‌ای یک بار، دستی هم بررسی کنید.
- اسکن کامل هارد را ماهانه انجام دهید؛ اسکن سریع روزانه.
- اگر از آنتی‌ویروس رایگان استفاده می‌کنید، اطمینان حاصل کنید که شامل محافظت زنده (**Real-time Protection**) باشد.
- اگر سیستم شما مشکوک است ولی آنتی‌ویروس چیزی پیدا نکرد، با یک ابزار مکمل مانند **Malwarebytes** یا **Emsisoft** اسکن کنید.

02

مراقب ایمیل‌های فریبنده باشید
هر پیوستی امن نیست

ایمیل فیشینگ، ساده‌ترین و مرگبارترین روش نفوذ است. هکر فقط باید شما را متقاعد کند که کلیک کنید. بقیه را بدافزار انجام می‌دهد.

چگونه فریب نخوریم؟

- نام دامنه را بررسی کنید: آیا واقعاً ایمیل از بانک شما آمده یا مثلاً از **bnk-secure.info**؟
- لحن ایمیل را بخوانید: آیا تهدیدآمیز، فوری یا عجیب است؟
- لینک را **Hover** کنید ولی کلیک نکنید: مقصد واقعی را ببینید.
- پیوست فایل‌های **.exe, .js, .vbs, .bat** و حتی **.docm** (ماکرو اکتیو) را باز نکنید.

توصیه پیشرفته‌تر:

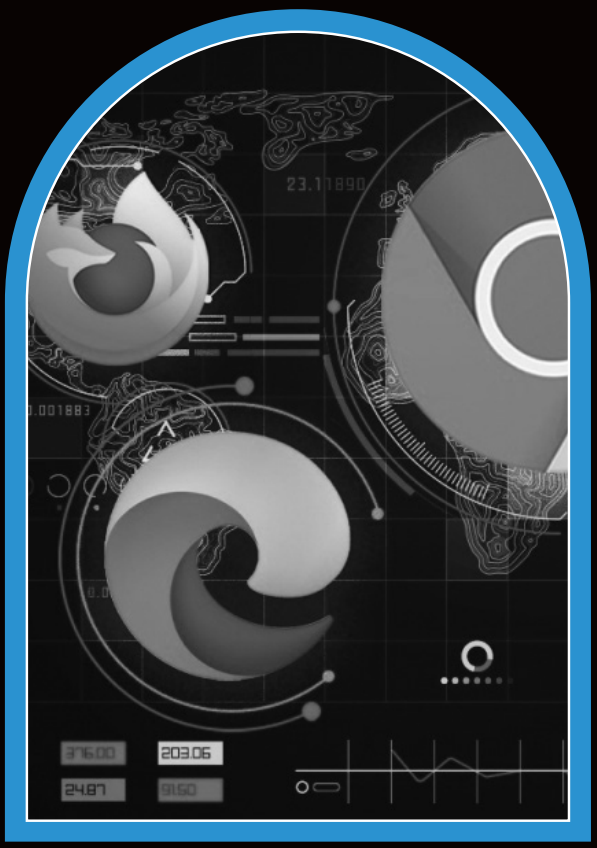
- از ابزارهای ایمیل‌سنجی مثل **MailScanner** یا **Mimecast** استفاده کنید.
- از **Gmail** یا سرویس‌های مشابه که سیستم تشخیص فیشینگ قوی دارند، بهره ببرید.

03

رفتار مرورگری خود را اصلاح کنید
هر سایت زیبایی امن نیست

یک وب‌سایت می‌تواند ویروس منتقل کند، حتی اگر بازدیدکننده منفعل باشید. بدافزارهایی مثل **drive-by download** بدون اینکه شما کلیکی کرده باشید، می‌توانند فایل آلوده دانلود کنند.

- چه کارهایی پرخطرند؟
  - کلیک روی تبلیغات هیجان‌انگیز: «شما برنده شدید!» یا «همین حالا لاغر شوید!»
  - باز کردن سایت‌هایی با دامنه‌های مشکوک یا کلمات عجیب در URL
  - استفاده از مرورگرهای قدیمی یا بدون افزونه امنیتی
- پیشنهاد کاربردی
  - مرورگر خود را به‌روزرسانی کنید.
  - از مرورگرهایی مثل Brave یا Firefox with uBlock Origin استفاده کنید.
  - فعال‌سازی Do Not Track و جلوگیری از اجرای خودکار JavaScript در سایت‌های ناشناس.



04

نرم‌افزارهای کرک‌شده
بزرگ‌ترین درب نفوذ

بسیاری از کاربران تصور می‌کنند که کرک کردن یک نرم‌افزار فقط برای دور زدن پول است. اما غافل‌اند که هکرها به‌راحتی فایل کرک را به Trojan آلوده می‌کنند و شما دروازه را خودتان باز می‌کنید!

- چرا این تهدید واقعی است؟
  - فایل‌های کرک معمولاً آنتی‌ویروس را غیرفعال می‌کنند.
  - هیچ بروزرسانی‌ای دریافت نمی‌کنید؛ باگ‌ها و آسیب‌پذیری‌ها باقی می‌مانند.
  - ابزارهای نظارتی (Remote Access Tools) مخفیانه نصب می‌شوند.
- جایگزین مناسب:
  - از نسخه‌های رایگان قانونی (Freeware) مثل LibreOffice یا GIMP استفاده کنید.
  - نسخه‌های آزمایشی Trial بسیاری از نرم‌افزارها نیاز شما را برطرف می‌کنند.

05

فلش USB آلوده
تهدید خاموش در جیب شما

فلش‌هـــا نه تنها اطلاعات حمل می‌کنند، بلکه ویروس هم منتقل می‌کنند. گروه‌های هکری پیشرفته بارها از فلش USB برای نفوذ استفاده کرده‌اند.

- اقدامات دفاعی:
  - قابلیت AutoRun را در ویندوز غیرفعال کنید.
  - فلش جدید را قبل از باز کردن، با آنتی‌ویروس اسکن کنید.
  - از باز کردن فایل‌هایی با نام‌های عجیب یا دو پسوند مثل invoice.pdf.exe بپرهیزید.

نکته مهم سازمانی: در شرکت‌ها، سیاست BYOD (Bring Your Own Device) باید محدود یا کنترل‌شده باشد.

06

پچ امنیتی
اهمیت آپدیت‌های مداوم را دست کم نگیرید

هکرها از آســیب‌پذیری‌های روز صفر (Zero-Day) اســتفاده می‌کنند، اما بیشــتر حملات به دلیل بی‌توجهی به آپدیت‌های ساده است.

- نکته قابل تأمل:

حمله باج‌افزار WannaCry فقط به‌دلیل یک باگ در SMB ویندوز انجام شــد که مایکروســافت قبلاً آن را رفع کرده بود.

- راهکار عملی:
  - تنظیمات Windows Update را روی «Automatic» بگذارید.
  - از ابزارهایــی مثل Patch My PC یا Ninite برای آپدیت اتوماتیک نرم‌افزارها استفاده کنید.

07

محدود کردن دسترسی‌ها
اصل کمترین مجوز (Least Privilege)

اگر هر کاربر دسترسی کامل به سیستم داشته باشد، بدافزار هم به همان اندازه آزاد خواهد بود.

- کاربرد این اصل:
  - کاربر عادی با دسترسی محدود وارد شود.
  - فقط در مواقع ضروری با **Admin** وارد شوید.
  - هر دستگاه **USB** یا نرم‌افزاری، دسترسی کامل به سیستم نداشته باشد.

08

امنیت موبایل
دستگاهی که همیشه همراه شماست

بسیاری از کاربران از موبایل غافل می‌شوند، در حالی که بیش از ۶۰٪ حملات هدفمند جدید، موبایلی هستند.

- توصیه‌ها:
  - از نصب **APK** خارج از **Google Play** اجتناب کنید.
  - مجوزهای اپلیکیشن‌ها را بازبینی کنید: چرا یک چراغ قوه به موقعیت مکانی شما نیاز دارد؟
  - آنتی‌ویروس موبایل مثل **Bitdefender Mobile** یا **Kaspersky Mobile** نصب کنید.

09

ابزارهای پایش سیستم
مراقب رفتارهای عجیب باشید

شناسایی بدافزار فقط با آنتی‌ویروس نیست. گاهی رفتار سیستم شما سرنخ‌هایی می‌دهد.

- نشانه‌های مشکوک:
  - روشن شدن فن سیستم بی‌دلیل
  - کند شدن ناگهانی سیستم
  - استفاده مشکوک از اینترنت در **Task Manager**
- ابزارهای حرفه‌ای:
  - ابزار **Sysinternals Suite**: بررسی پردازش‌ها، رجیستری، **startup**
  - ابزار **GlassWire**: پایش ترافیک شبکه
  - ابزار **Autoruns**: مدیریت آیتم‌های خودراه‌انداز

10

نسخه پشتیبان
آخرین سنگر دفاعی شما

بدافزارهایی مثل باج‌افزار، غیرقابل برگشت‌اند. اگر نسخه پشتیبان نداشته باشید، ممکن است همه‌چیز را از دست بدهید.

- توصیه‌ها:
  - پشتیبان‌گیری (بکاپ) منظم و زمان‌بندی‌شده تنظیم کنید (روزانه یا هفتگی)
  - بکاپ را روی هارد اکسترنال یا فضای ابری امن ذخیره کنید
  - بکاپ را رمزنگاری کنید و به‌صورت آفلاین نگه دارید

CONCLUSION

نتیجه‌گیری

امنیت سایبری مثل بهداشت شخصی است. نمی‌شود فقط یک بار رعایتش کرد. باید همیشه، هر روز، در هر لحظه به آن توجه کنیم. رعایت همین ۱۰ اصل، جلوی بیشتر حملات را می‌گیرد. اما فراموش نکنید: هکرها همیشه روش‌های جدید پیدا می‌کنند، و شما هم باید همیشه یک قدم جلوتر باشید.

بخش ویژه

بدافزارهای موبایلی تهدیدی در جیب شما

تا همین چند سال پیش، بدافزارها فقط تهدیدی برای لپ‌تاپ و کامپیوترهای رومیزی بودند. اما امروز، گوشی‌های هوشمند ما به کامپیوترهایی قدرتمند تبدیل شده‌اند؛ همراه با اطلاعات شخصی، عکس‌های خصوصی، حساب‌های بانکی، پیام‌ها، و حتی کلیدهای ورود به دنیای دیجیتال. بدافزارهای موبایلی دقیقاً به همین دلیل جذاب شده‌اند: دسترسی ۲۴ ساعته، بدون آنتی‌ویروس، و اغلب بدون دانش فنی کاربر. این بخش، به بررسی دقیق این تهدید روبه‌رشد می‌پردازد.

چگونه گوشی‌های هوشمند آلوده می‌شوند؟

بدافزارهای موبایلی از مسیرهای مختلفی وارد گوشی شما می‌شوند. برخلاف تصور رایج، حتی باز نکردن فایل‌های عجیب هم تضمین امنیت نیست.

رایج‌ترین روش‌های آلوده‌سازی گوشی:

- نصب اپلیکیشن از منابع نامعتبر:

بیش از ۹۰٪ بدافزارهای موبایلی از طریق فایل‌های APK آلوده نصب می‌شوند که خارج از Google Play یا App Store دریافت شده‌اند.

- کلیک روی لینک‌های فیشینگ در پیامک یا پیام‌رسان‌ها:

لینک‌هایی که وانمود می‌کنند شما جایزه برده‌اید یا نیاز به تایید حساب دارید، ممکن است اپی مخفیانه نصب کنند یا مجوزهایی را به طور خودکار فعال کنند.

- شبکه‌های وای‌فای عمومی و جعلی:

اگر در کافی‌شاپ یا فرودگاه به شبکه‌ای متصل شوید که هکر کنترل آن را دارد، می‌تواند اپ‌های مخرب را از راه دور در گوشی شما نصب کند یا اطلاعات را شنود کند.

- استفاده از کابل شارژ عمومی (Juice Jacking):

برخی بدافزارها از طریق پورت USB آلوده در ایستگاه‌های شارژ عمومی منتقل می‌شوند.

- بدافزارهای پنهان در بازی‌های رایگان یا اپ‌های پرکاربرد:

حتی در Google Play یا App Store، گاهی اپ‌هایی منتشر می‌شوند که ظاهری قانونی دارند ولی به‌مرور رفتار مخرب بروز می‌دهند (مثلاً دسترسی به میکروفون یا ارسال پیام‌های تبلیغاتی بدون اطلاع).

- برنامه‌های مشکوک خارج از Google Play یا App Store دانلود و نصب اپ از منابعی به‌جز فروشگاه‌های رسمی بزرگ‌ترین نقطه ضعف امنیتی کاربران است.

چرا منابع غیررسمی خطرناک‌اند؟

- هیچ بررسی امنیتی انجام نمی‌شود: Google Play و App Store مکانیزم‌های اسکن بدافزار دارند (مثل Google Play Protect).
- اپلیکیشن می‌تواند کاملاً جعلی باشد: ظاهر اپ ممکن است دقیقاً مثل نسخه رسمی باشد ولی در واقع یک برنامه جاسوس‌افزار باشد.
- مجوزها به‌صورت پنهان دریافت می‌شوند: فایل‌های APK می‌توانند بدون اطلاع کاربر به اطلاعات مخاطبین، پیامک‌ها، دوربین و میکروفون دسترسی پیدا کنند.

نشانه‌هایی که باید هشدار دهند:

- سایت‌هایی که ادعا می‌کنند نسخه «کرک‌شده» یا «VIP» اپ‌ها را ارائه می‌کنند.
- اپ‌هایی با نام مشابه نسخه رسمی اما با پسوندهای متفاوت مثل .gold, .mod, .pro.

نشانه‌های آلودگی گوشی به بدافزار

بسیاری از کاربران اصلاً متوجه آلودگی نمی‌شوند. در اینجا، علائمی را مرور می‌کنیم که باید به آن‌ها حساس باشید:

- کندی ناگهانی گوشی یا داغ شدن غیرعادی
- نمایش تبلیغات ناخواسته حتی وقتی هیچ اپی باز نیست
- افزایش مصرف باتری یا دیتا بدون دلیل واضح
- ارسال پیامک به مخاطبین بدون اطلاع شما
- اپ‌هایی که خودبه‌خود نصب شده‌اند یا حتی در لیست اپ‌ها مخفی هستند
- قطع شدن آنتی‌ویروس یا غیرفعال شدن Google Play Protect
- شنیدن صدای عجیب یا روشن شدن ناگهانی میکروفون/دوربین

اگر حتی یک مورد از این نشانه‌ها را مشاهده کردید، بهتر است گوشی خود را بررسی و ایمن‌سازی کنید.

روش‌های پاکسازی گوشی آلوده به بدافزار

اگر مشکوک هستید که گوشی‌تان آلوده شده، این مراحل را دنبال کنید:

گام اول: حالت Safe Mode را فعال کنید

در این حالت، فقط اپ‌های سیستم اجرا می‌شوند و اپ‌های شخص ثالث غیرفعال می‌گردند.

- نحوه فعال‌سازی:

در اکثر گوشی‌های اندرویدی: دکمه پاور را نگه دارید > لمس طولانی روی «Power Off» > گزینه «Safe Mode»

در iOS: نیاز به ریست کامل یا بررسی از طریق تنظیمات > حریم خصوصی > Analytics

گام دوم: حذف اپ‌های مشکوک

- به بخش تنظیمات > اپ‌ها بروید و هر اپ ناشناسی را حذف کنید.
- اگر گزینه حذف غیرفعال بود، ابتدا دسترسی مدیریتی (Device Admin Access) آن را غیرفعال کنید.

گام سوم: استفاده از آنتی‌ویروس موبایلی قوی

نرم‌افزارهایی مانند:

- Bitdefender Mobile Security
- Kaspersky Mobile
- ESET Mobile
- Malwarebytes Mobile

این اپ‌ها نه‌فقط بدافزار را پاک می‌کنند، بلکه رفتارهای پنهان را نیز رصد می‌کنند.

گام چهارم: ریست کارخانه (در صورت لزوم)

- اگر هیچ‌کدام از راهکارهای بالا جواب نداد، ریست کامل گوشی به حالت کارخانه توصیه می‌شود.
- قبل از آن حتماً از اطلاعات مهم بک‌آپ بگیرید.

اقدامات پیشگیرانه برای آینده

- اپلیکیشن را فقط از فروشگاه رسمی نصب کنید.
- گزینه «Install from Unknown Sources» را غیرفعال نگه دارید.
- به مجوزهایی که اپ درخواست می‌کند توجه کنید؛ چرا یک ماشین‌حساب به میکروفون نیاز دارد؟
- از آنتی‌ویروس‌های موبایلی استفاده کنید و آن را به‌روز نگه دارید.
- دستگاه را رمزگذاری کنید و از قفل صفحه ایمن (پین، الگو یا بیومتریک) استفاده نمایید.
- Google Play Protect را روشن نگه دارید.

اقدامات پیشگیرانه
در برابر حملات بدافزارها

پیشگیری از بدافزارها فقط با نصب آنتی‌ویروس ممکن نیست. مجموعه‌ای از عادت‌ها، تنظیمات و رفتارهای دیجیتال باید رعایت شوند تا سیستم شما امن بماند. این چک‌لیست راهنمایی است برای تمام کاربران – چه در خانه و چه در محل کار – تا با انجام اقدامات ساده ولی مؤثر، جلوی فاجعه را بگیرند.

استفاده از آنتی‌ویروس به‌روز – خط دفاع اول شما

هـر کامپیوتر یا موبایلی که به اینترنت متصل می‌شـود، باید مجهز به آنتی‌ویروس فعال و به‌روز باشد.

اقدامات ضروری:

آنتی‌ویروس معتبر (رایگان یا پولی) نصب شده است

به‌روزرسانی خودکار فعال است

قابلیت محافظت همزمـان (Real-time Protection) روشن است

اسکن کامل سیستم هفته‌ای یک بار انجام می‌شود

نسخه موبایلی آنتی‌ویروس برای گوشی نیز فعال شده است

پیشنهاد ابزار:

Bitdefender – Kaspersky – Malwarebytes – ESET – Windows Defender

عـدم کلیـک روی لینک‌هـای ناشـناس – یـک کلیک، کافی‌ست برای فاجعه

لینک‌های مشکوک در ایمیل، پیامک یا پیام‌رسان‌ها، دروازه‌ی ورود بدافزارها هستند.

نکات عملیاتی:

- لینک‌های ایمیل‌های ناشناس را باز نمی‌کنم

- قبل از کلیک، لینک را Hover می‌کنم تا مقصد واقعی را ببینم
- اگر پیام از طرف بانک یا شرکت رسمی است، ابتدا وارد سایت رسمی می‌شوم
- به لینک‌هایی با دامنه عجیب (مثلاً xyz.biz یا offer-win.ru) شک دارم
- پیام‌های فوری با محتوای: «همین الان کلیک کن»، «جایزه بردی!» را نادیده می‌گیرم

پیشنهاد فنی:

- استفاده از ابزارهای تحلیل لینک مثل VirusTotal یا CheckPhish.ai

گرفتن نسخه پشتیبان به‌صورت منظم – بیمه‌نامه‌ی دیجیتال

- وقتی باج‌افزار فایل‌هایتان را گروگان می‌گیرد، فقط یک نسخه پشتیبان می‌تواند نجات‌بخش باشد.

چک‌لیست پشتیبان‌گیری:

- هفته‌ای یک بار از فایل‌های مهم پشتیبان می‌گیرم
- پشتیبان را روی هارد اکسترنال یا فضای ابری امن نگه می‌دارم
- نسخه پشتیبان به سیستم اصلی وصل نیست (در برابر آلودگی باج‌افزار مقاوم است)
- از ابزارهای حرفه‌ای پشتیبان‌گیری استفاده می‌کنم (Acronis, Macrium Reflect, Cobian Backup)
- فایل‌های پشتیبان رمزگذاری شده‌اند (در صورت سرقت فیزیکی)

توصیه کلیدی:

حداقل دو نسخه پشتیبان داشته باشید: یکی آنلاین، یکی آفلاین.

رمزگذاری فایل‌های حساس – حفظ محرمانگی حتی در هنگام سرقت

رمزگذاری، فایل‌های شما را در برابر دسترسی غیرمجاز محافظت می‌کند، حتی اگر فایل به‌دست مهاجم بیفتد.

نکات کاربردی:

- فایل‌های محرمانه‌ی کاری را رمزگذاری می‌کنم
- از ابزارهایی مثل VeraCrypt یا BitLocker برای رمزگذاری دیسک استفاده می‌کنم
- فایل‌های حساس در فضای ابری، رمزگذاری شده آپلود می‌شوند
- ایمیل‌های حاوی اطلاعات حساس را با رمز عبور یا لینک‌های موقت ارسال می‌کنم

نکته امنیتی:

حتی در صورت آلوده شدن سیستم، رمزگذاری مانع دسترسی بدافزار به محتوای حساس می‌شود.

آموزش کاربران – دیوار انسانی امنیت

بزرگ‌ترین ضعف امنیتی، بی‌اطلاعی کاربران است. هکرها اغلب از خطای انسانی سوءاستفاده می‌کنند.

اقدامات آموزشی:

- آموزش فیشینگ و بدافزار به کارمندان داده شده
- نمونه پیام‌های مشکوک و سناریوهای جعلی برای تمرین در اختیار آن‌ها قرار گرفته
- اطلاعیه‌های هفتگی یا ماهانه‌ی امنیتی به کاربران ارسال می‌شود
- کاربران می‌دانند چطور رفتار مشکوک را گزارش کنند

پیشنهاد محتوا:

پادکست، موشن‌گرافی، آزمون دانشی، بروشور امنیتی

کنترل دسترسی‌ها – هر کسی، هر چیزی را نبیند

بدافزارها وقتی به فایل یا سیستمی دسترسی نداشته باشند، نمی‌توانند کاری کنند. کنترل دسترسی یعنی تعیین اینکه چه کسی، به چه چیزی، در چه زمانی دسترسی دارد.

نکات حیاتی:

- برای هر فرد، فقط دسترسی لازم و ضروری تعریف شده
- اشتراک‌گذاری پوشه‌ها یا درایوها در شبکه به‌صورت محدود انجام شده
- اطلاعات طبقه‌بندی‌شده فقط برای کاربران مجاز در دسترس است
- دسترسی‌ها به‌صورت دوره‌ای بازبینی و حذف می‌شود

استفاده از حساب‌های کاربری با حداقل سطح دسترسی

استفاده از حساب Admin برای فعالیت‌های روزمره مثل وب‌گردی یا نصب نرم‌افزار، دروازه طلایی ورود بدافزارهاست.

چک‌لیست سطوح دسترسی:

- برای کارهای معمول از حساب Standard استفاده می‌کنم
- حساب Admin فقط برای نصب یا تغییر تنظیمات سیستمی استفاده می‌شود
- اکانت Admin رمز عبور پیچیده و متفاوت دارد
- کاربران مهمان یا غیرمجاز در سیستم تعریف نشده‌اند

نکته امنیتی:

اگر بدافزار از طریق حساب محدود وارد شود، نمی‌تواند تغییرات سیستمی عمیق ایجاد کند.

چک‌لیست پیشگیری، راهکار نهایی نیست، اما ستون اصلی دفاع است

اگر حتی نیمی از این چک‌لیست در محیط کاری یا شخصی شما رعایت شود، می‌توان از ۹۰٪ تهدیدات بدافزاری جلوگیری کرد. امنیت سایبری ترکیبی از ابزار، دانش و رفتار است. این چک‌لیست نقطه شروعی برای یک رفتار دیجیتال مسئولانه است.

SCENARIO

سناریو ...

فایل آلوده در ایمیل فقط یک کلیک کافی بود

شخصیت داستان: علی – کارمند مالی پرتلاش، اما بی‌خبر
علی رضایی، ۳۴ ساله، کارمند واحد مالی شرکت «توسعه‌گران آینده»، مثل همیشه ساعت ۸:۱۵ پشت سیستم‌اش نشست. قهوه‌اش را جرعه‌ای نوشید و Outlook را باز کرد. مثل همیشه، پر از ایمیل‌های کاری، فاکتورها، نامه‌های بانکی و مکاتبات روزانه.

در میان ایمیل‌ها، یک پیام با موضوع رسمی توجه‌اش را جلب کرد:

- فرستنده: support@parsibank-info.com
- موضوع: تغییر در شماره حساب مقصد – اقدام فوری
- پیوست: xlsm.۲۰۲٤_AccountUpdate

علی، بدون لحظه‌ای تردید، فایل اکسل را باز کرد.

اجرای فایل – آغاز فاجعه

فایل باز شـد. صفحه‌ای با لوگوی بانک و جدولی از شـماره حسـاب‌های جدید نمایش داده شد. هیچ‌چیز مشکوکی نبود، جز یک پیام کوچک در بالا:

«برای مشاهده اطلاعات جدید، ماکروها را فعال کنید.»

علـی روی دکمـه‌ی «Enable Content» کلیک کرد. هیچ اتفاق خاصی نیفتاد. جدول همان بود. کمی مشکوک شد، اما چون عجله داشت، آن را بست و سراغ کار بعدی رفت...

اما پشت پرده، همه‌چیز شروع شده بود.

مرحله اول: نصب بدافزار – بی‌صدا، بی‌نشانه

با فعال شـدن ماکرو، کد VBA داخل فایل اجرا شد. این کد وظیفه‌اش مشخص بود:

- تمـاس با یک سـرور فرماندهی (C۲) از طریق پروکسـی اینترنت شرکت
- دانلود بدافزاری از نوع loader به‌نام BazarLoader
- اجرای کدهای مخرب در حافظه (بدون ذخیره روی دیسک (Fileless

در کمتر از ۲ دقیقه، سیستم علی به یک پلتفرم کنترل از راه دور برای مهاجم تبدیل شد.

مرحله دوم: گسترش در شبکه – مثل آتش در انبار کاه

مهاجم حالا درون شـبکه بود. بـا اسـتفاده از ابزارهایی مثل Mimikatz، اطلاعـات احـراز هویت علی و چنـد کاربر دیگر را اسـتخراج کرد. سپس با استفاده از دسترسی‌ها، بین سیستم‌های مختلف جابه‌جا شد.

در کمتر از ۲ ساعت:

- بخش مالی
- واحد منابع انسانی
- سیستم حسابداری ابری

همگی آلوده شدند.

در سـاعت ۱۱:۳۰، مهاجم با باج‌افزار LockBit ضربه نهایی را وارد کرد.

مرحله سوم: قفل شدن سیستم‌ها – سکوت، سپس وحشت

کارمندان یکی‌یکی تماس می‌گرفتند:

فایل‌هام باز نمی‌شن!

سیسـتم هنگ کرده، فقط یه صفحه سـیاهه که نوشته: Your files are encrypted

سرور مالی بالا نمیاد!

ساعت ۱۲:۰۵، تیم IT متوجه ماجرا شد. اما دیگر دیر شده بود. سیسـتم‌ها خاموش، فایل‌ها رمزگذاری‌شده، و پیامی روی هر سیستم:

Your files have been encrypted by LockBit."
۱۵ To recover them, contact us via TOR and pay BTC."

واکنش تیم IT در میانه‌ی یک بحران

واحد فناوری اطلاعات (IT) وارد حالت بحران شد. اقداماتی که انجام دادند:

اقدامات فوری:

- قطع تمام سیستم‌ها از شبکه داخلی و اینترنت
- فعال‌سازی کانال اضطراری ارتباط (تلفن و پیامک)
- بررسی نقاط ورودی (با تمرکز روی ایمیل علی)
- اسکن کامل لاگ‌های سرور Exchange
- اطلاع‌رسانی به مدیریت و واحد حقوقی

مشکلات کلیدی:

- پشـتیبان‌گیری کامل نبود؛ آخرین بک‌آپ مربوط به ۲۰ روز پیش بود
- سیسـتم‌های آنتی‌ویروس بدون EDR، توانایی تشـخیص فعالیت fileless را نداشتند
- کاربـران آموزش‌دیده نبودند؛ علی فکر می‌کرد «ماکرو» چیز بی‌خطر است

پیامدهای مالی و سازمانی

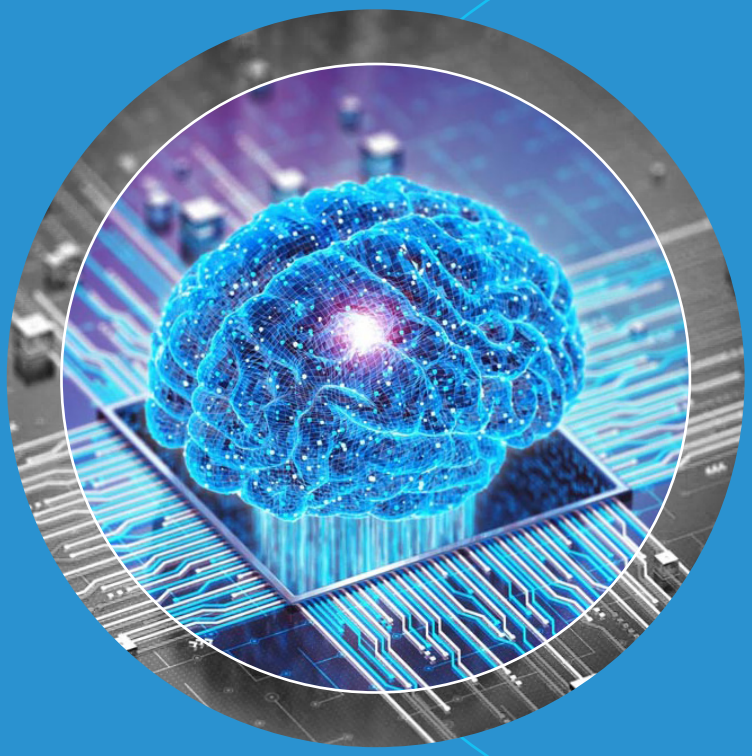
- دو روز تعطیلی کامل سیستم‌های سازمانی
- تعویق پرداخت حقوق بیش از ٤۰۰ نفر
- خسارت مستقیم مالی: حدود ۹۵۰ میلیون تومان
- خسـارت اعتباری: از دسـت رفتن اعتماد مشتریان و انتشار شایعات در فضای مجازی
- تلاش برای بازیابی فایل‌ها با تیم IR، بدون پرداخت باج

این فقط یک داستان نیست؛ این روایت تکراری هزاران حمله واقعی در شرکت‌های کوچک و بزرگ دنیاست.

درس‌هایی که باید بگیریم:

- هر فایل پیوستی امن نیست، حتی اگر از طرف بانک باشد.
- آموزش امنیت دیجیتال باید بخشی از فرهنگ سازمان باشد.
- پشتیبان‌گیری منظم، تنها راه بازیابی اطلاعات است.
- استفاده از آنتی‌ویروس پیشرفته با قابلیت تشخیص رفتاری و EDR حیاتی است.
- ایمیـل همچنان بزرگ‌ترین درگاه ورود تهدید اسـت. آن را جدی بگیرید.

KNOWLEDGE GAME



بازی دانشی

آیا امنیت دیجیتال خود را می‌شناسید؟

هر سؤال را با دقت بخوانید و گزینه‌ای را انتخاب کنید که بیشترین تطابق با رفتار واقعی شما دارد.
در پایان، امتیاز خود را جمع بزنید و ببینید در کجای مسیر امنیت دیجیتال هستید!

سؤال یک:
وقتی ایمیلی دریافت می‌کنید که ظاهراً از طرف بانک است و یک لینک دارد، چه کار می‌کنید؟
A) بلافاصله روی لینک کلیک می‌کنم چون فکر می‌کنم بانک درست می‌فرسته (۰)
B) کمی مکث می‌کنم ولی بازش می‌کنم چون کنجکاوم (۱)
C) لینک را بررسی می‌کنم، اگر عجیب بود باز نمی‌کنم (۲)
D) اصلاً روی هیچ لینکی کلیک نمی‌کنم و مستقیماً به سایت بانک می‌رم (۳)

سؤال دو:
از چه نوع رمز عبور برای حساب‌های اینترنتی‌تان استفاده می‌کنید؟
A) رمز ساده و یکسان برای همه جا (۰)
B) رمز نسبتاً پیچیده ولی مشابه برای چند حساب (۱)
C) رمزهای مختلف ولی یادداشت‌شده روی کاغذ یا گوشی (۲)
D) رمزهای قوی و منحصربه‌فرد با استفاده از Password Manager (۳)

سؤال سه:
آیا رمز دومرحله‌ای (2FA/MFA) برای حساب‌های مهم مثل ایمیل یا شبکه اجتماعی فعال کرده‌اید؟
A) نه، هیچ‌وقت (۰)
B) فقط برای یکی دو تا از حساب‌هام (۱)
C) برای بیشتر حساب‌هام (۲)
D) برای همه حساب‌های مهم (۳)

سؤال چهار:
در صورت دریافت فایل پیوست از فرستنده ناشناس چه می‌کنید؟
A) باز می‌کنم ببینم چی فرستاده (۰)
B) با آنتی‌ویروس چک می‌کنم و بعد باز می‌کنم (۱)
C) فقط اگر فرمت قابل اعتماد داشت باز می‌کنم (۲)
D) نمی‌کَنم بازش کنم، حذفش می‌کنم (۳)

سؤال پنج:
هر چند وقت یک‌بار از اطلاعات مهم خود نسخه پشتیبان تهیه می‌کنید؟
A) هیچ‌وقت (۰)
B) فقط زمانی که احساس خطر کنم (۱)
C) ماهی یک‌بار (۲)
D) به‌طور منظم، به صورت زمان‌بندی‌شده (۳)

سؤال شش:
وقتی در یک کافی‌شاپ یا فرودگاه به وای‌فای عمومی وصل می‌شوید، چه کار می‌کنید؟
A) مستقیم وارد حساب‌های مهم می‌شوم (۰)
B) فقط پیام چک می‌کنم، بانک نه (۱)
C) از VPN استفاده می‌کنم (۲)
D) به شبکه عمومی اصلاً وصل نمی‌شوم (۳)

سؤال هفت:
از کجا اپلیکیشن موبایل نصب می‌کنید؟
A) هر سایتی که لینک بده (۰)
B) از فروشگاه‌های رسمی، ولی گاهی خارج از آن هم (۱)
C) فقط Google Play یا App Store (۲)
D) علاوه بر فروشگاه رسمی، اپ رو با آنتی‌ویروس هم اسکن می‌کنم (۳)

سؤال هشت:
در مرورگر شما چند افزونه امنیتی نصب است؟
A) نمی‌دونم افزونه چیه (۰)
B) یکی دوتا تصادفی نصب کردم (۱)
C) از افزونه‌هایی مثل uBlock Origin یا HTTPS Everywhere استفاده می‌کنم (۲)
D) افزونه امنیتی نصب کرده‌ام و تنظیمات امنیت مرورگر را بهینه کرده‌ام (۳)

سؤال نه:
آیا تاکنون قربانی بدافزار یا حمله فیشینگ شده‌اید؟
A) بله، چند بار! (۰)
B) یک بار اتفاق افتاد (۱)
C) خیر، اما موارد مشکوک دیدم (۲)
D) هرگز، چون همیشه مراقب هستم (۳)

سؤال ده:
در محل کار یا خانه، رمز وای‌فای شما چگونه است؟
A) هنوز هم admin یا ۱۲۳۴۵۶ه! (۰)
B) رمز ساده‌ای گذاشتم، ولی عوض کردم (۱)
C) رمز قوی گذاشتم، ولی بین چند نفر مشترکه (۲)
D) رمز قوی و منحصربه‌فرد دارم، با مک آدرس فیلترینگ فعال (۳)

نحوه امتیازدهی:
برای هر گزینه‌ای که انتخاب کردید، امتیاز آن را یادداشت کنید و در پایان، امتیازها را جمع بزنید. (حداکثر ۳۰)

تفسیر نتایج:
۰ تا ۹ امتیاز: میدون مین! شما شدیداً در معرض خطر هستید. احتمال اینکه قربانی فیشینگ، بدافزار یا سرقت اطلاعات شوید بسیار بالاست. لطفاً فوراً سطح آگاهی خود را بالا ببرید!

۱۰ تا ۱۹ امتیاز: امنیت حداقلی. شما برخی اصول را می‌دانید، اما رعایت نمی‌کنید یا فقط به‌صورت ناقص اجرا می‌کنید. یک حمله جدی می‌تواند شما را هدف بگیرد. آموزش ببینید و رفتارهای خود را اصلاح کنید.

۲۰ تا ۲۶ امتیاز: کاربر آگاه. شما رفتارهای خوبی دارید، اصول مهم را رعایت می‌کنید و خطرات را تا حد زیادی کاهش داده‌اید. با کمی تقویت در ابزارهای فنی و پشتیبان‌گیری، سطح امنیتتان بسیار بالا خواهد رفت.

۲۷ تا ۳۰ امتیاز: کاربر حرفه‌ای امنیت دیجیتال. شما نه تنها آگاه هستید، بلکه در سطح یک کارشناس عمل می‌کنید. ابزارها، رفتارها و پیشگیری‌ها را به‌درستی به‌کار گرفته‌اید. نمونه‌ای برای دیگران هستید!