راهکار مدیریت امن انتقال فایل برنا

Malware Detection

Cloud Air Gap

Zero Trust Architecture

مرکز نوآوری و شتابدهی برنا

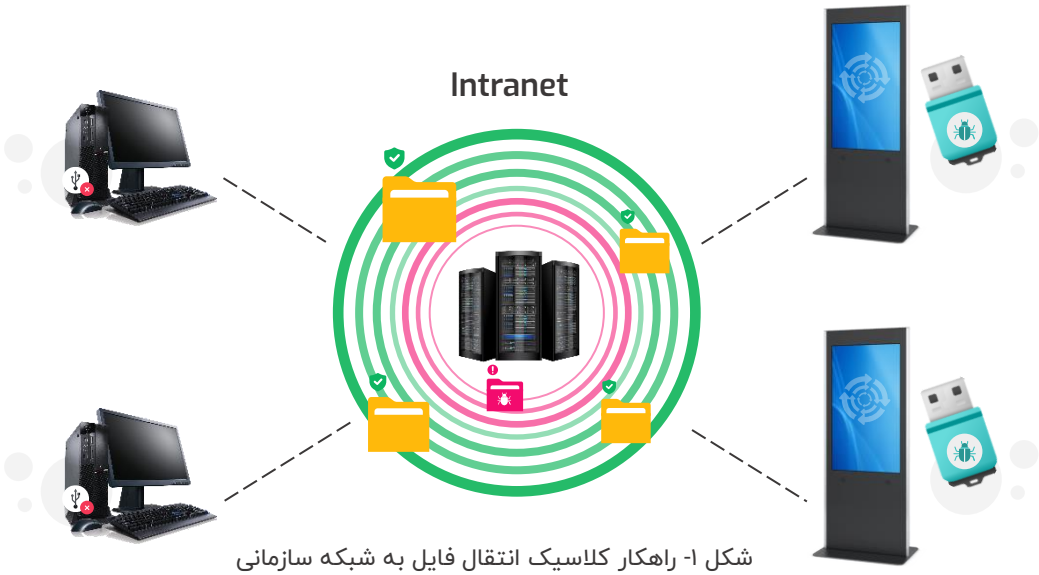
INNOVATION BRIDGE

مقدمه

ورود فایل‌های آلوده به بدافزار می‌تواند موجب نفوذ به سازمان یا آسیب به زیرساخت‌های نرم‌افزاری و سخت‌افزاری شود. یکی از مسائلی که در سازمان‌های بزرگ دولتی، نظامی و سازمان‌هایی که شبکه‌های اطلاعاتی داخلی (اینترانت) دارند، موضوع انتقال فایل از طریق دستگاه‌های قابل حمل، نظیر فلش مموری‌ها و هاردهای اکسترنال از شبکه‌های نامطمئن[۱] به شبکه‌های مطمئن[۲] است.

انتقال بدافزارها به درون سازمان به واسطه فایل‌های آلوده، همواره یکی از چالش‌های مهم سازمان‌ها است. برای رفع این چالش می‌توان از راهکارهای کلاسیک Multi-AV که از کیوسک‌های سخت‌افزاری و نرم‌افزاری بهره می‌گیرند استفاده کرد.

راهکارهای کلاسیک موجود (شکل ۱)، پس از اسکن فایل و اطمینان از عدم آلودگی، فایل‌ها را به شبکه داخلی سازمان انتقال می‌دهند، این در حالی است که فایل‌ها ممکن است آلوده به بدافزاری باشند که در زمان ورود آن به سازمان، راهکارهای Mulit-AV قادر به شناسایی آن‌ها نباشند. بنابراین آلودگی می‌تواند وارد سازمان شده و به عنوان داده‌ی قابل اعتماد به دفعات مورد بهره‌برداری قرار گیرد یا ممکن است فایل بدون آلودگی وارد سازمان شده و آسیب‌پذیری به‌صورت داخلی به آن تزریق شود. این موضوع مغایر با معماری Zero-Trust[۳] است و راهکارهای کیوسک سنتی قادر به بررسی فایل‌ها پس از ورود به سازمان نیستند.



شکل ۱- راهکار کلاسیک انتقال فایل به شبکه سازمانی

[۱] Untrust

[۲] Trust

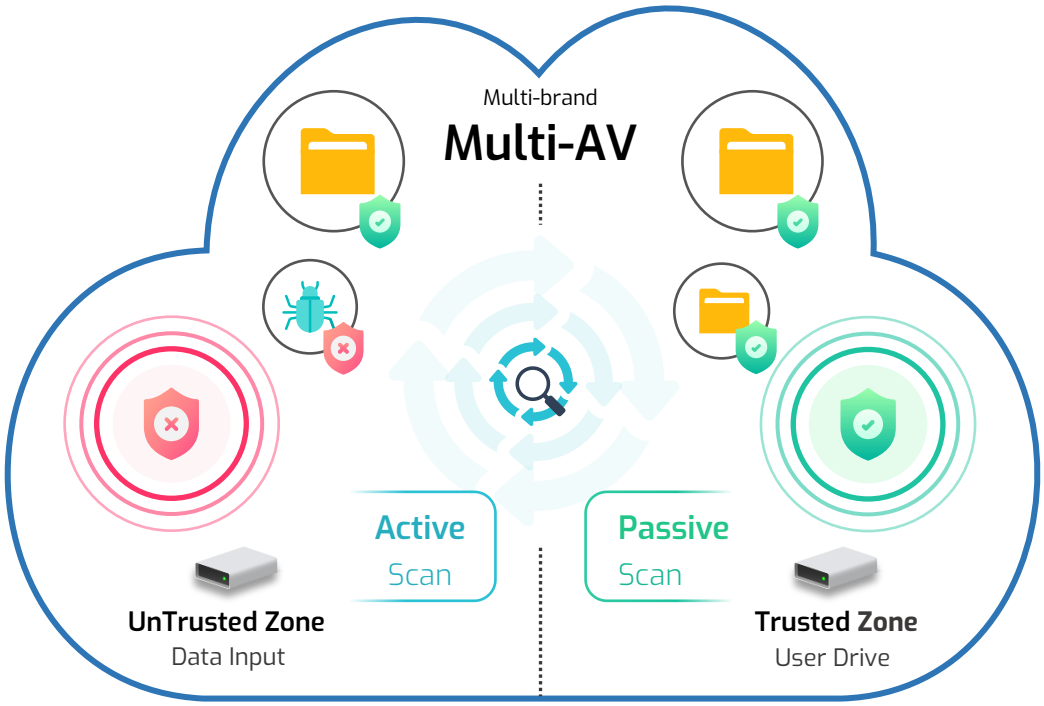
[۳] در شبکه‌های Zero-Trust فرض بر این است که همواره مهاجمان در داخل و خارج از شبکه وجود دارند.

معرفی راهکار مدیریت امن انتقال فایل برنا

راهکار مدیریت امن انتقال فایل برنا، با هدف انتقال امن و قابل نظارت داده‌ها بین شـــبکه‌های نامطمئن و مطمئن، تسهیل و تسریع تبادل داده‌ها برای کاربران بین دو شبکه و ایجاد سازوکاری برای ورود و خروج داده‌ها به صورت امن در نظر گرفته شده است. این راهکار مبتنی بر معماری Zero-Trust بوده و جایگزینی برای روش‌های کلاسیک انتقال فایل در سازمان‌هایی که شبکه‌های Air-Gap دارند است (شکل ۲).

تفاوت کلیدی این راهکار با روش‌های کلاسیک در این است که هرگز به اسکن‌های اولیه اعتماد نمی‌شود و فایل‌ها حتی بعد از اطمینان از آلوده نبودن به بدافزار و ورود به شـــبکه‌های داخلی ســـازمان، جهت جلوگیری از گســـترش آلودگی احتمالی کشف نشده در زمان ورود، همواره مورد بررسی و اسکن مجدد قرار می‌گیرند. این راهکار با استقرار موتورهای تحلیل بدافزار به صـــورت Multi-Brand باعث کاهش ریســـک‌های تجاری و فنی با یک برند، اســـتاندارد شـــدن زیرساخت‌های تحلیل بدافزار سازمان، کاهش ریسک‌های مرتبط با تاخیر در فرآیندهای به روز رسانی، کاهش ریسک باگ‌های احتمالی در موتور اصلی تحلیل بدافزار، کاهش ریسک خطاهای برنامه‌نویسی و مدیریت استثناء در برندهای مختلف می‌شود.

این سامانه با بهره‌گیری از اسکن‌های چندلایه توسط موتورهای تحلیل بدافزار به صورت پویا[۴] (در زمان ورود فایل‌ها به ســازمان) و انفعالی[۵] (بعد از ورود فایل‌ها به ســازمان) ســطح امنیتی از لحاظ آلوده بودن به بدافزار را ارتقا می‌بخشـــد. همچنین با امضای دیجیتال فایل‌ها اصالت آن‌ها را از نظر موتور تحلیل بدافزار مشخص می‌نماید.



شکل ۲- معماری راهکار مدیریت امن انتقال فایل برنا

[۴] Active

[۵] Passive

مزایای راهکار مدیریت امن انتقال فایل برنا

- پشتیبانی از سه برند بیت بان، سایبرنو و گراف در حال حاضر
- استاندارد شدن زیرساخت‌های تحلیل بدافزار مستقل از یک برند خاص
- کاهش ریسک‌های تجاری مرتبط با یک برند (نظیر Vendor lock-in)
- کاهش ریسک مرتبط با تاخیر در فرآیندهای به روز رسانی
- کاهش ریسک باگ‌های احتمالی در موتور اصلی تحلیل بدافزار
- کاهش ریسک خطاهای برنامه‌نویسی و مدیریت موارد استثناء در برندهای مختلف
- امکان ارایه گزارش‌های Confusion Matrix جهت بنچمارک
- مدیریت دسترس‌پذیری داده‌ها

در شکل ۳ قابلیت پیکربندی راهکار مدیریت امن انتقال فایل برنا در سطوح مختلف نشان داده شده است. مثلاً در لایه لبه برای تسریع در انتقال فایل می‌توان از پیکربندی‌های سبک‌تر و متناسب با استانداردهای امنیتی سازمان و در سطوح بعدی از اسکن‌های پیشرفته‌تر با تعداد آنتی‌ویروس‌های بیشتر استفاده کرد. همچنین با استفاده از تحلیل‌های پویا، هوش مصنوعی و یادگیری ماشین روی بارکاری می‌توان رفتارهای ناهنجار را شناسایی نمود، که این می‌تواند موجب ارتقای ضریب امنیتی شود. در شکل ۳ یک نمونه از پیکربندی این راهکار در سطوح مختلف نشان داده شده است.

Deep – Level 3	Deep – Level 2 (34)	Deep – Level 1 (22)	Quick (10)	Quick (5)	Quick (0)
	Benign list	Benign list	Benign list	Benign list	Benign list
	Black list	Black list	Black list	Black list	Black list
	YARA2 / NSRL	YARA2 / NSRL	YARA1 / NSRL	YARA1 / NSRL	YARA / NSRL
	Windows Defender	-	Windows Defender	Windows Defender	
	ClamAV	ClamAV	ClamAV	ClamAV	
	Avira	-	Avira	Avira	
	McAfee	McAfee	McAfee	McAfee	
	AhnLab-V3	-	AhnLab	AhnLab	
	BitDefender	BitDefender	BitDefender		
	ESET-NOD32	ESET	ESET		
	Kaspersky	Kaspersky	Kaspersky		
	Sophos	-	Sophos		
	-	-	EMSISoft		
	Padvish	Padvish			
	Gdata / ESCAN / Comodo / DrWeb / Fsecure / QuickHeal	Gdata / eScan / Comodo / DrWeb / Fsecure / QuickHeal			
	Avast, AVG, Emsisoft, GData ,Ikarus, K7AntiVirus, Symantec, Fortinet				
Thread Intelligence (TI)					
Dynamic Analysis & Sandbox					
Workload Analysis using AI/ML					

شکل ۳- پیکربندی اسکنرها در سطوح مختلف در راهکار برنا

ویژگی‌های سامانه مدیریت امن انتقال فایل برنا و مقایسه آن با راهکارهای موجود

ردیف	عنوان	راهکارهای کلاسیک	راهکار برنا
۱	پشتیبانی از موتورهای تحیل بدافزار به صورت Multi-Brand	×	✓
۲	تعداد موتور تحلیل بدافزار	+۱۰	+۴۵
۳	بررسی فایل با دیتابیس فایل های آلوده شناخته شده	✓	✓
۴	پشتیبانی از پیمایش سریع در کیوسک به صورت Active	✓	✓
۵	گزارش های پایه از وضعیت بدافزار در سطح سازمان	✓	✓
۶	نظارت و کنترل دسترسی ریزدانه بر روی اسناد	×	✓
۷	گزارش مصرف داده‌ها (فایل های پرمصرف)	×	✓
۸	تولید لاگ در سطوح مختلف با ریزدانگی بالا	×	✓
۹	پشتیبانی از پیمایش عمیق و پویا به صورت Passive	×	✓
۱۰	شناسایی فایل های تغییریافته در محیط مطمئن	×	✓
۱۱	اسکن مجدد اشیای تغییریافته به صورت Passive	×	✓
۱۲	پشتیبانی از LDAP و AD در سمت کاربر نهایی	✓	✓
۱۳	تنوع روش های ورود داده از محیط نامطمئن	+۲	+۴
۱۴	تنوع روش‌های خروج داده از محیط مطمئن	۱+	+۷
۱۵	کیوسک وب در سمت اینترنت برای ورود داده‌ها	✓	✓
۱۶	کشف الگوی استفاده از فایل‌های آلوده در سطح سازمان	×	✓
۱۷	ارائه گزارش‌های Confusion Matrix	×	✓
۱۸	کشف ناهنجاری در بار کاری شبکه ذخیره سازی	×	✓
۱۹	امضای دیجیتال نتیجه اسکن توسط Multi-AV	×	✓
۲۰	مدیریت افزونگی داده‌ها و نرخ تکرار	×	✓
۲۱	دسترس پذیری داده‌ها	×	% ۹۹/۹
۲۲	قابلیت یکپارچه‌سازی با Nextcloud	✓	✓
۲۳	مقیاس‌پذیری خطی فضای ذخیره‌سازی (PAYG[۶])	×	✓
۲۴	قابلیت انتقال حجم انبوه داده به صورت Batch	✓	✓
۲۵	امکان مدیریت متمرکز فایل‌های قرنطینه شده	×	✓
۲۶	قابلیت انقضای فایل‌ها	×	✓
۲۷	قرنطینه فایل‌های آلوده	×	✓
۲۸	پشتیبانی از نسخه‌های مختلف یک فایل	×	✓
۲۹	پشتیبانی از کاربران در محیط اینترنت و اینترانت	محدود	بدون محدودیت
۳۰	مبتنی بر معماری Zero-Trust	×	✓

[۶] Pay as you Grow

مرکز نوآوری و شتابدهی برنا

INNOVATION BRIDGE

۰۲۱-۲۸۴۲۲۹۱۰ ، ۰۲۱-۸۶۰۹۶۱۷۸

sales@burna.ir

www.burna.ir

تهران، خیابان کارگر شمالی، خیابان شانزدهم، پارک علم و فناوری دانشگاه تهران، ساختمان شماره۳،

شرکت صنایع الکترونیک زعیم