کاتالوگ محصول
سیستم‌کال

سندباکس تحلیل بدافزار: اجرای فایل روی ویندوز
جدا، و گرفتن IOC از همان اجرا.

systemcall.ir

sandbox.systemcall.ir

PRODUCT CATALOG · 2026

سندباکس سیستم‌کال چه کار می‌کند

فایل روی کامپیوتر تحلیل‌گر باز نمی‌شود. داخل یک ویندوز جدا اجرا می‌شود و همان اجرا دسکتاپ، درخت پردازه، فایل، رجیستری، PCAP و در صورت نیاز دامپ حافظه را نگه می‌دارد. نتیجه و امتیاز برای این است که بدانید اول کدام فایل را نگاه کنید. مخرب‌بودن را از رابطهٔ پردازهٔ والد و فرزند، خط فرمان، مسیر فایل ساخته‌شده و مقصد شبکه می‌فهمید.

وقتی آنتی‌ویروس‌ها با هم اختلاف دارند، یا پیوست ایمیل مشکوک است، فایل را اینجا اجرا می‌کنید و IOC و تکنیک ATT&CK را برمی‌دارید. جلوگیری روی خود سیستم کار EDR است. اسکن لینک در سیستم‌کال نیست؛ ورودی فقط فایل است.

ورودی تسک

قبل از شروع، مدت اجرا، نسخهٔ ویندوز و این را مشخص می‌کنید که اینترنت این ویندوز وصل باشد یا نه. هش SHA-256 و منبع فایل (تیکت، ایمیل، سیستم) جدا از ویندوز اجرا ثبت می‌شود. خود فایل را بعد از تحلیل در چت نفرستید؛ لینک همان اجرا و بازپخش کافی است. پوشهٔ مشترک بین ویندوز تحلیل و سیستم میزبان باز نمی‌ماند.

خواندن نتیجه

اولین پردازهٔ غیرعادی را روی درخت پیدا کنید، بعد همان بازه را در رجیستری و شبکه بگردید. Run key، فایل داخل AppData یا Temp، و DNS/TLS همان پردازه معمولاً همان چیزی است که به فایروال و detection می‌رود. اگر نمونه به‌خاطر شناسایی VM یا timeout ساکت مانده، در یادداشت تسک بنویسید رفتار ناقص است. اسنپ‌شات مهمان بعد از نمونهٔ مخرب به نقطهٔ تمیز برمی‌گردد تا رویداد اجرای قبل داخل baseline نماند.

کجا مصرف می‌شود

SOC برای triage پیوست و آلارم. MSSP برای اینکه خروجی تسک‌ها یک شکل باشد. DFIR برای استخراج شاخص قبل از scoping روی لاگ محیط. در لاب Blue Team همان recording با کارآموز مرور می‌شود، بدون اینکه نمونه روی لپ‌تاپ شخصی بیاید.

لایه‌های همان تسک

دسکتاپ

تصویر مهمان با پروکسی VNC داخل مرورگر می‌آید و فریم‌های session برای replay ذخیره می‌شود. ISO و LNK و dropper چندمرحله‌ای اغلب یک کلیک UI دارند که در لاگ پردازه دیده نمی‌شود. بازپخش را با timestamp رویدادها میزان کنید تا معلوم شود کدام پنجره هم‌زمان با ساخت پردازه یا اولین DNS بوده.

شبکه و PCAP

کوئری IP، TLS، HTTP، DNS، پورت و follow استریم روی ترافیک مهمان است و PCAP جدا دانلود می‌شود. دامنه‌ای را IOC کنید که به پردازهٔ مشکوک چسبیده باشد. ترافیک telemetry ویندوز و آپدیت را از لیست خارج کنید. برای بلوکه، دامنهٔ اختصاصی با TTL کوتاه قابل دفاع‌تر از IP ابری اشتراکی است. SNI و الگوی زمانی را در یادداشت تسک بیاورید حتی اگر payload رمز شده باشد.

حافظه

اگر drop پاک شده یا کد به پردازهٔ دیگر رفته، روی دیسک چیزی نمی‌ماند. از همان پردازه دامپ بگیرید و رشته، hex و YARA را روی دامپ بزنید. ناحیهٔ RWX بدون image، ماژول unbacked و هدر PE تزریق‌شده شاهد T1055 است. دامپ پردازه با acquisition کامل RAM یکی نیست.

پردازه، فایل، رجیستری

روی درخت، مسیر باینری و command line را بخوانید. winword به cmd و بعد powershell -enc، کپی به AppData، و مقدار Run/RunOnce در HKCU یا HKLM الگوی پرتکرار است. rundll32 و msiexec و certutil را فقط وقتی والد و آرگومان غیرعادی است مشکوک حساب کنید. نام پردازهٔ شبیه سرویس ویندوز در مسیر کاربر را با مسیر واقعی چک کنید.

Static و خوشهٔ نمونه

نوع فایل، import، entropy و YARA قبل از detonation مشخص می‌کند نمونه packed است یا نه. قاعدهٔ YARA را روی corpus تمیز هم اجرا کنید وگرنه روی installerهای عادی hit می‌دهد. برای ربط دو نمونه، SHA-256 را ملاک نگیرید. مسیر drop، نام mutex، دامنه و شکل کلید Run را کنار هم بگذارید و تا قبل از تکرار شاهد، برچسب خانوادهٔ عمومی نزنید.

خروجی تسک و دسترسی

چه چیزی از تسک خارج می‌شود

Score و verdict روی خود تسک است. برای کنترل‌ها این‌ها را جدا کنید: SHA-256 باینری و drop، دامنه و IP با پردازهٔ مولد، مسیر فایل، نام مقدار Run، و تکنیک ATT&CK همراه با شاهد همان دقیقه. خروجی Sigma و نتیجهٔ YARA از artifact همان اجرا گرفته می‌شود. IOC بدون confidence و بدون تاریخ انقضا وارد بلاک‌لیست دائمی نشود.

دسترسی تحلیل‌گر و API

تاریخچه، stop، تمدید زمان، تگ و مقایسهٔ دو تسک داخل کنسول است. Lookup و feed تهدید، قانون YARA کاربر، و preset اجرا هم همان‌جاست. API نسخهٔ ۱ با Bearer token نمونه می‌گیرد و وضعیت، IOC، گراف پردازه، PCAP و فریم replay را برمی‌گرداند. رویداد زنده روی WebSocket است و کانال VNC با همان احراز هویت باز می‌شود. توکن را داخل ریپازیتوری نگذارید.

وقتی رفتار ناقص است

Timeout کوتاه، قطع شبکه، یا anti-VM باعث می‌شود loader بعد از چند ثانیه خارج شود و C2 دیده نشود. این را در تسک بنویسید. اگر اسنپ‌شات مهمان به حالت پایه برنگردد، فایل و کلید رجیستری اجرای قبلی با نمونهٔ جدید قاطی می‌شود. آپدیت ویندوز وسط دو مقایسه هم همین کار را با baseline می‌کند.

یادداشت برای همکار بعدی

خلاصه را کوتاه بنویسید: نمونه از کجا آمده، زنجیرهٔ پردازه، یک یا دو IOC شبکه، تکنیک دیده‌شده، و اینکه اجرا کامل بوده یا نه. اسکرین بدون زمان و لیست T-code بدون رویداد، به detection engineer چیزی برای کوئری SIEM نمی‌دهد.

دسترسی

کنسول عملیاتی sandbox.systemcall.ir است. برای اکانت سازمانی از systemcall.ir/demo درخواست بدهید. این فایل فقط شرح capability است. detonation داخل آزمایشگاه انجام می‌شود.