دانلود چک‌لیست ChaosBot و راهنمای پیکربندی EDR

1. مقدمه

این سند مجموعه‌ای از اقدامات عملی، تنظیمات نظارتی و کوئری‌های شکار تهدید (Threat Hunting) است تا تیم‌های امنیتی بتوانند در برابر بدافزار **ChaosBot** به‌سرعت واکنش نشان دهند. محتوای این راهنما بر اساس رفتارهای شناخته‌شده این خانواده بدافزار (PowerShell abuse, DLL sideloading, Discord-based C2) تهیه شده و هدف آن کاهش زمان تشخیص (MTTD) و زمان پاسخ (MTTR) است.

2. خلاصه تهدید(Executive Summary)

- ✓ **نام تهدید:** ChaosBot
- ✓ **ویژگی‌ها:** مبتنی برRust ، استفاده از Discord برایC2 ، تکنیک‌های LNK phishing و DLL sideloading، قابلیتETW tampering ، اجرای PowerShell رمزگذاری‌شده، ایجاد.reverse proxy
- ✓ **مخاطب هدف:** سازمان‌های دارای کاربران زیاد، سازمان‌های مالی و خدماتی، محیط‌هایی که از مرورگرها و پیام‌رسان‌های دسکتاپی استفاده می‌کنند.

3. چک‌لیست فوری(Actionable 48-hour checklist)

الف) شناسایی و مسدودسازی(Detect & Contain)

- ☐ فعال‌سازی و اجرای اسکن EDR رویendpoint های حساس (متمرکز بر LNK وDLL)
- ☐ به‌سرعت جستجو در SIEM برای الگوهای اجرای PowerShell عجیب (مثلاً پارامترهایenc- ، nop-، - w hidden)
- ☐ مسدودسازی موقت ترافیک خروجی به دامنه‌ها/IPهای ناشناس مرتبط با Discord API (با دقت: دقت ترافیک قانونی را بررسی کنید).
- ☐ جلوگیری از بارگذاری DLL از مسیرهای کاربری غیرمعمول در مرورگرها (Policyیا Application Control).

ب) بررسی و شکار(Hunt)

- [ ] اجرای کوئری‌های Hunting (بخش ۵) در Splunk/ELK و ذخیره نتایج.
- [ ] بررسی لاگها برای تغییرات در رجیستری (Run/RunOnce/Services) و ایجاد تسک‌های زمان‌بندی‌شده.
- [ ] شناسایی ماشین‌هایی که ETW یا PowerShell logging آنها غیرفعال شده.

ج) تقویت و پیشگیری(Prevent)

- [ ] الزامی کردن MFA برای حساب‌های حساس (ادمین، VPN، سرویس‌ها).
- [ ] اعمال محدودیت اجرای PowerShell (Constrained Language Mode) یا اجرای قوانین AppLocker/WDACبرایendpoint های حساس.
- [ ] بروزرسانی و سخت‌سازی مرورگرها و حذف کتابخانه‌های غیرضروری در مسیرهای بارگذاریDLL .

د) بازیابی و مستندسازی(Recover & Report)

- [ ] تهیه نسخه کامل و آفلاین از بکاپ‌های حیاتی و تست بازیابی.
- [ ] ثبت کامل زنجیره حمله و زمان‌بندی رخدادها (Timeline) برای تحلیل‌های بعدی و گزارش مدیریت.
- [ ] اطلاع‌رسانی داخلی به تیم‌های مرتبط و آماده‌سازی اطلاع‌رسانی به کاربران در صورت نیاز.

4. پیکربندی پیشنهادی EDR (تفضیلی)

4.1تنظیمات عمومی

- ✓ فعال‌سازی **Behavioral Detection**با تمرکز روی اجرای اسکریپت‌ها و رفتارهای-post exploitation.

- ✓ فعال‌سازی **Real-time File Integrity Monitoring** روی مسیرهای AppData ، Program Files و مسیرهای Launch.

4.2 قواعد پیشنهادی (Rules)

- ✓ **Rule A — PowerShell Suspicious Execution :**
  - Trigger : اجرای `powershell.exe` با پارامترهای `-w hidden, -nop, -enc` یا فراخوانی از مسیرهای موقت.(`%APPDATA%, %TEMP%`)
  - Action : block execution (در صورت سیاست) quarantine فایل، alert به SOC.
- ✓ **Rule B — DLL Sideloading from User Paths :**
  - Trigger : ImageLoad events برای DLL های بارگذاری‌شده از مسیرهای کاربر مانند `AppData\Local\*` که نام‌های مشابه `msedge_elf.dll` دارند.
  - Action: alert + snapshot process memory + collect loaded modules.
- ✓ **Rule C — ETW Tampering Detection :**
  - Trigger : خاموش یا تغییر در ETW providers مرتبط با PowerShell, ImageLoad, Registry changes.
  - Action : بالا بردن اولویت به Incident, forensics snapshot.
- ✓ **Rule D — Discord C2 Behavioral Indicator :**
  - Trigger : فرآیندهایی که به API ها یا Endpoint های متعلق به Discord متصل می‌شوند در حالی که فرآیند اصلی آنها مرورگر/PowerShell است.
  - Action: alert, throttle network, collect network metadata.

4.3 جمع‌آوری لاگ‌ها (Log Sources)

- ✓ Process creation (Sysmon EventID 1)
- ✓ Image load events (Sysmon EventID 7)
- ✓ PowerShell logging (Operational & ScriptBlock logging)
- ✓ Windows Registry changes (EventID 13/12 بسته به Sysmon)

- ✓ Network connection events (DNS, proxy logs, firewall)

5.کوئری‌های — Hunting نمونه برای Splunk وSigma

5.1 Splunk نمونه کوئری پایه

```
index=security sourcetype=Sysmon
(
  (Image="*\\powershell.exe" AND CommandLine="*-enc*" )
  OR
  (ImageLoaded="*msedge_elf.dll" OR
ImageLoaded="*\\AppData\\Local\\Microsoft\\Edge\\*")
)
| stats count by host, Image, CommandLine, ImageLoaded, _time
| where count > 0
```

5.2 Detect Discord-related PowerShell calls. Splunk

```
index=security sourcetype=Sysmon Image="*\\powershell.exe"
| search CommandLine="*discord*" OR CommandLine="*api.discordapp.com*"
| table _time host user Image CommandLine ParentImage
```

5.3 Sigma rule (نمونه مفهومی)

```
title: Suspicious PowerShell Using Discord C2 Indicators
id: a1b2c3d4-xxxx-xxxx-xxxx-xxxxxxxx
description: Detect PowerShell executions that reference Discord or Discord-
related endpoints.
status: experimental
author: YourSOC
detection:
  selection:
    Image|endswith: '\powershell.exe'
    CommandLine|contains:
      - 'discord'
      - 'api.discordapp.com'
  condition: selection
level: high
```

نکته: کوئری‌ها را با شاخص‌ها و نام‌های فیلدهای محیط SIEM خودتان تطبیق دهید وFalse Positive ها را بررسی کنید.

6. فرآیند پاسخ به حادثه(IR Playbook: ChaosBot)

مرحله ۰ — فعال‌سازی تیم و اعلام وضعیت

- ✓ اعلام وضعیت Incident به تیم IR و تعیینIncident Commander .
- ✓ فعال‌سازی کانال‌های ارتباطی امن (مثلاً Slack یا Teams Channel اختصاصی با دسترسی محدود).

مرحله ۱ — شناسایی و محدودسازی(Identify & Contain)

- ✓ اجرای کوئری‌های Hunting رویSIEM ، جداسازیhost (isolation) های مشکوک از شبکه.(EDR)
- ✓ مسدودسازی ارتباطات خروجی مشکوک در فایروال و پروکسی.

مرحله ۲ — جمع‌آوری شواهد(Forensics)

- ✓ گرفتن snapshot حافظه (memory dump) و تصویر دیسک ازendpoint های مشکوک.
- ✓ جمع‌آوری Sysmon logs, PowerShell logs, Etw logs و network PCAP در صورت امکان.

مرحله ۳ — حذف و پاکسازی(Eradicate)

- ✓ حذف فایل‌های مخرب، پاک‌سازی اتصالات persistence (Registry, Scheduled Tasks, Services).
- ✓ ریست پسوردهای حساب‌های سرویس آسیب‌دیده و بررسی دسترسی‌هایSSO/MFA .

مرحله ۴ — بازیابی(Recover)

- ✓ Restore از بکاپ‌های امن پس از اطمینان از پاکی تصاویر.
- ✓ مانیتور مضاعفhost ها برای ۷–۱۴ روز پس از بازگردانی.

مرحله ۵ — تحلیل پس از حادثه(Post-incident)

- ✓ تولید گزارش کامل شامل timeline ، root cause analysis، توصیه‌های اصلاحی.
- ✓ به‌روزرسانی Playbook و قواعد EDR بر اساس یافته‌ها.

IOC.7 ها (Indicators of Compromise) —جدول فنی

دسته	نمونه/مقدار	توضیحات
File path	`C:\Users\<user>\AppData\Local\Microsoft\Edge\msedge_elf.dll`	DLLجعلی برای sideloading
File path	`C:\Users\<user>\AppData\Roaming\Discord\Update\discord_updater.exe`	استیجر masquerading as Discord updater
Process / CommandLine	`powershell.exe -nop -w hidden -enc <Base64>`	اجرای اسکریپت رمزگذاری شده
Registry	`HKCU\Software\Microsoft\Windows\CurrentVersion\Run\DiscordHelper`	persistence autostart key
Task	`schtasks /create /tn "UpdateService" /tr "<path>" /sc onlogon`	scheduled task persistence
Network	`api.discordapp[.]com` (یا الگوهای مشابه)	استفاده از Discord APIبرای C2
Log artefact	ETW Providers disabled	تلاش برای طعمه‌زدایی و پنهان‌سازی

توصیهIOC: ها را همیشه به فرمت مناسب (CSV, STIX) تبدیل و در سیستم‌های TIP/TI خود آپلود کنید.

8. نقشه‌برداری به MITRE ATT&CK (نمونه)

- ✓ **Initial Access (T1193)** — Spearphishing Attachment (LNK)
- ✓ **Execution (T1059.001)** — PowerShell
- ✓ **Persistence (T1053)** — Scheduled Task
- ✓ **Privilege Escalation (T1068)** —احتمالی (بسته به payload)
- ✓ **Defense Evasion (T1070, T1562)** — ETW tampering, DLL sideloading
- ✓ **Command and Control (T1071.001)** — Web Protocols (Discord API)
- ✓ **Exfiltration (T1041)** — Exfil via C2 channel (Discord)

9. توصیه‌های بازیابی(Remediation & Recovery)

- ✓ پاکسازی کاملendpoint های آلوده یا بازسازی سیستم از تصویر سالم(golden image) .
- ✓ بازنشانی رمز عبور برای حساب‌های احتمالی تحت تاثیر و فعال‌سازیMFA .
- ✓ بررسی و تقویت سیاست‌های پشتیبان‌گیری (آفلاین وair-gapped backups)
- ✓ اجرای آموزش امنیتی برای کاربران در خصوص پیوست‌های LNK و پیام‌های فیشینگ.

پایان — نکات اجرایی نهایی

۱. این سند را به‌عنوان یک فایل PDF ذخیره کنید و در مخزن مستندات محرمانه تیم قرار دهید.
۲. کوئری‌ها را متناسب با فیلدها و شاخص‌های محیط SIEM خود اصلاح کنید.
۳. پس از هر حادثه، Playbook و قواعد EDR را بازبینی کرده و نسخه جدید را منتشر کنید.