📌 گزارش اطلاعاتی–سایبری

موضوع: ارزیابی ادعای بازداشت «سرکرده گروه هکری Backdoor» مرتبط با «لب‌دوختگان» توسط سازمان اطلاعات سپاه
نویسنده: یاسمین حنیفه طباطبایی – پژوهشگر امنیت سایبری، تحلیلگر تهدیدات، متخصص شبکه، رمزنگاری و امنیت اطلاعات
طبقه‌بندی: تحلیل تخصصی – عمومی‌سازی‌شده
تاریخ: نوامبر ۲۰۲۵

۱. مقدمه

در روزهای اخیر، سازمان اطلاعات سپاه (ساس) اعلام کرد که «سرکرده گروه هکری Backdoor» را که آن را مرتبط با گروه لب‌دوختگان و «شبکه‌های اسرائیلی» معرفی می‌کند، بازداشت کرده است. این خبر با انتشار یک مستند تلویزیونی در رسانه‌های رسمی جمهوری اسلامی همراه شد که در آن ادعاهایی درباره نحوه شناسایی، عملیات سایبری، و وابستگی این گروه مطرح شد.

این گزارش یک تحلیل فنی–اطلاعاتی مستقل است که بر اساس داده‌های عملیاتی، الگوهای رفتار تهدید (TTP)، شواهد ساختاری، و تجربه عملی در حوزه امنیت سایبری و ردگیری مالی–دیجیتال تهیه شده است.

۲. ارزیابی کلی ادعاها

با توجه به الگوی سال‌های گذشته در پرونده‌های مشابه (نظیر گروه لب‌دوختگان و سایر عملیات سایبری یا ضدحکومتی شناخته‌شده)، تحلیل تخصصی نشان می‌دهد که:

1. بخش عظیمی از شناسایی و بازداشت‌ها ناشی از خطاهای OPSEC افراد بوده است.
2. ترسیم مسیرهای مالی و ردیابی تراکنش‌های رمزارزی یکی از اصلی‌ترین ابزارهای شناسایی بوده است.
3. مستندهای امنیتی منتشرشده به‌طور معمول بیش از حد امنیتی‌سازی شده و فاقد جزئیات فنی واقعی‌اند.
4. پیوست‌های تصویری و انیمیشن‌های نمایش‌داده‌شده معمولاً مبتنی بر واقعیت فنی نیستند.

این گزارش تلاش می‌کند روایت امنیتی رژیم را از زاویه‌ای فنی، بی‌طرفانه و مبتنی بر تجربه میدانی تحلیل کند.

۳. روش‌های محتمل شناسایی (Technical Attribution Vectors)

۳.۱. ردگیری رمزارز (Cryptocurrency Traceback)

احتمالاً کلیدی‌ترین نقطه شکست اپراتوری همین بخش بوده است.

- استفاده از والت‌های قابل ردیابی
- تراکنش‌های چرخه‌ای (cyclical transfers)
- استفاده از سرویس‌هایی با KYC اجباری
- ورود به اکسچنج‌های داخلی یا خارجی با IP ایران
- دریافت منابع مالی از کانال‌های غیرمخفی

ردگیری رمزارز در ایران:
سازمان اطلاعات سپاه (ساس), طی سال‌های گذشته با همکاری صرافی‌های داخلی، داده‌های KYC، شماره کارت‌ها، IP لاگ‌ها، و Device-Fingerprint را در اختیار داشته و این موضوع امکان «De-anonymization» را فراهم می‌کند.

۳.۲. خطاهای رایج OPSEC

رایج‌ترین الگوهای شکست امنیت عملیاتی:

- استفاده هم‌زمان از ابزارهای شخصی و عملیاتی
- تغییر نکردن الگوهای رفتاری در کار و زندگی
- ورود به پلتفرم‌های حساس بدون VPN پایدار
- نشت اطلاعات از طریق حساب‌های شبکه اجتماعی
- حمل گوشی‌های شخصی به محل کار عملیاتی

۳.۳. ارتباطات دیجیتال

هکرهایی که از: تلگرام, واتس‌اپ, دیسکورد, روبیکا/ایتا (در صورت اشتباه) استفاده می‌کنند، معمولاً تحت خطر **Metadata Correlation** قرار می‌گیرند:

- ساعت فعالیت
- الگوی پاسخ‌دهی
- همپوشانی جغرافیایی
- شماره‌های ذخیره‌شده یا هم‌پوشان

۳.۴. نفوذ انسانی (HUMINT Integration)

در بسیاری از پرونده‌های قبلی دیده شده که: دوستان نزدیک, همکاران, هم‌خانه‌ها, ارتباطات احساسی یا خانوادگی, به‌طور فعال مورد بازجویی یا تطمیع قرار گرفته‌اند و اطلاعات کلیدی را منتقل کرده‌اند.

۴. تحلیل قابلیت‌ها و ضعف‌های رژیم در حوزه فنی

بر اساس بررسی‌های فنی:

توانمندی‌های واقعی سپاه
- دسترسی گسترده به داده‌های مخابراتی
- دسترسی به KYC صرافی‌ها و بانک‌ها
- تجهیزات شنود قانونی و غیرقانونی
- توانایی محدود در تحلیل بلاک‌چین
- استفاده از شرکت‌های فین‌تک وابسته برای جمع‌آوری اطلاعات

توانمندی‌هایی که اغلب اغراق می‌شود
- توانایی پیچیده در بهره‌برداری از Zero-Dayها
- توانایی انجام Attribution سطح NSA
- تسلط کامل بر ابزارهای ضدناشناس‌سازی مانند Tor-Deanonymization
- پیاده‌سازی عملیات چندلایه بدون کمک انسانی

۵. تحلیل مورد «گروه بک دور» Backdoor Group

بر اساس الگوهای بیان‌شده در مستندهای قبلی و مدل فعالیت مجموعه‌های مشابه، محتمل‌ترین مسیر شناسایی:

۵.۱. زنجیره احتمالی شناسایی
1. تحلیل تراکنش‌های رمزارزی
2. به‌دست آوردن یک آدرس KYCشده
3. استخراج IP لاگ‌ها
4. Cross-Referencing با داده‌های مخابراتی
5. شناسایی دستگاه مورد استفاده
6. شناسایی شبکه اجتماعی، دوستان، الگوهای رفتاری
7. دستگیری فیزیکی

۵.۲. نشانه‌های ساختگی و تبلیغاتی
- استفاده از انیمیشن‌های غیرواقعی در مستند
- عدم ارائه نمونه واقعی از Tools یا Scripts
- تکرار ادعاهای «ارتباط با اسرائیل» بدون شاهد
- مبالغه در توانایی‌های تکنیکی گروه
- ادعای «شبکه گسترده» بدون ارائه ساختار عملیاتی

۶. جمع‌بندی (Assessment)

بر اساس تحلیل امنیت سایبری و داده‌های شناخته‌شده:

🔵 **احتمال واقعی:**
این فرد یا گروه از طریق **تراکنش‌های رمزارزی، خطاهای OPSEC و همپوشانی داده‌های دیجیتال** شناسایی شده‌اند.

🔴 **احتمال ساختگی/تبلیغاتی:**
ادعاهای «شبکه اسرائیلی»، «نفوذ گسترده در سامانه‌های حساس»، «عملیات پیچیده سایبری»، بیش از حد بزرگ‌نمایی و فاقد شواهد فنی‌اند.

🟢 **ارزیابی نهایی:**
این دست بازداشت‌ها بیشتر نتیجه‌ی **ترکیب اشتباهات عملیاتی افراد، تسلط سپاه بر داده‌های مالی–مخابراتی، و تبلیغات امنیتی** است تا کشف‌های پیچیده سایبری.