Bitdefender

آناتومی APT چینی که نهادهای دولتی جنوب شرقی آسیا را هدف قرار می‌دهد

ابزارها و روش‌های بهره‌جویی:

- فایل‌های Signed binary،
Backdoor را در حافظه دانلود می‌کنند.
- از سرورهای DC آلوده برای کنترل شبکه استفاده می‌کنند.
- از ابزارهای متداول برای اکتشاف و استخراج داده‌ها استفاده می‌شود.

آلوده‌گی بیش از ۲۰۰ ماشین:

زیرساخت حمله به احتمال زیاد هنوز فعال است.

۳ Backdoor بکار گرفته‌شده در سرور کنترل و فرمان‌دهی:

(FunnyDream و PCShare ،Chinoxy)

اهداف احتمالی APT:

- علاقه‌مند به زیرساخت‌های امنیت ملی کشورها
- جاسوسی صنعتی
- مستندات حساس و حیاتی

پیشگیری

ضد بدافزار
تشخیص و مسدودسازی
هر سه نوع RAT

بازرسی فرآیند
تشخیص و مسدودسازی
در مرحله اجرا

شناسایی

اجرا
هشداردهی براساس ۷ تکنیک
MITRE منحصربه‌فرد

دفاع از شبکه
شناسایی و مسدودسازی
سرور کنترل و فرمان‌دهی

ماندگاری
هشداردهی براساس ۷ تکنیک
MITRE منحصربه‌فرد

دورزدن سیستم‌های امنیتی
هشداردهی براساس ۴ تکنیک
MITRE منحصربه‌فرد

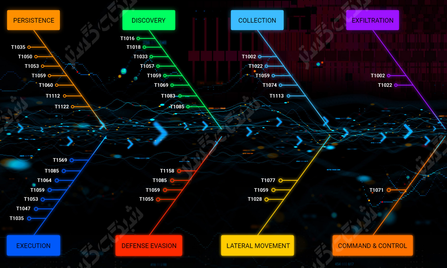
جمع‌آوری
هشداردهی براساس ۵ تکنیک
MITRE منحصربه‌فرد

توسعه دامنه آلودگی
هشداردهی براساس ۳ تکنیک
MITRE منحصربه‌فرد

اکتشاف
هشداردهی براساس ۸ تکنیک
MITRE منحصربه‌فرد

کنترل و فرمان‌دهی
هشداردهی براساس ۱ تکنیک
MITRE منحصربه‌فرد

سرقت و استخراج اطلاعات
هشداردهی براساس ۲ تکنیک
MITRE منحصربه‌فرد



چارچوب MITRE ATT&CK که مخفف Adversarial Tactics, Techniques, and Common Knowledge بوده و توسط MITRE Corporation ارائه شده یک پایگاه‌داده‌ش در حال رشد است که تاکتیک‌ها و تکنیک‌های مهاجمان را براساس حملات مشاهده شده در دنیای واقعی شناسایی نموده و در دسترس همگان قرار می‌دهد.
این چارچوب هم برای مهاجمان و هم برای مدافعان سایبری قابل فهم بوده و در موقعیت‌های بسیاری مثل تشخیص نفوذ، شکار تهدید، مهندسی امنیت، هوش تهدید و مدیریت ریسک مورد استفاده قرار می‌گیرد.

مکانیزم‌ها و تکنیک‌های MITER ATT&CK بکارگرفته شده در کارزار APT چینی:

- T1002 – Data Compressed
- T1016 – System Network Configuration Discovery
- T1018 – Remote System Discovery
- T1022 – Data Encrypted
- T1028 – Windows Remote Management
- T1033 – System Owner/User Discovery
- T1035 – Service Execution
- T1047 – Windows Management Instrumentation
- T1050 – New Service
- T1053 – Scheduled Task
- T1055 – Process Injection
- T1057 – Process Discovery
- T1059 – Command-Line Interface
- T1060 – Registry Run Keys / Start Folder
- T1064 – Scripting
- T1069 – Permission Groups Discovery
- T1071 – Standard Application Layer Protocol
- T1074 – Data Staged
- T1077 – Windows Admin Shares
- T1083 – File and Directory Discovery
- T1085 – Rundll32
- T1112 – Modify Registry
- T1113 – Screen Capture
- T1122 – Component Object Model Hijacking
- T1158 – Hidden Files and Directories
- T1569 – System Services

منبع: Bitdefender Labs Draco Team Whitepaper, Dessecting a Chinese APT Trageting South Eastern Asian Government Institutions
۲۷ آبان ۱۳۹۹

شبکه گستر
امنیت شما | وظیفه ما
تهران خیابان ظفر ۲۷۳
تلفن ۴۲۰۵۳۲ - ۰۲۱
www.shabakeh.net
اتاق اخبار newsroom.shabakeh.net
مرکز آموزش events.shabakeh.net
مرکز پشتیبانی my.shabakeh.net