APTs

Advanced and Persistent Threats

Uma visão geral de um problema tecnológico e geopolítico

Gabriel Ferrari Wagnitz - gabriel@wagnitz.com.br

O QUE SÃO?

Hackers financiados por estados-nação

Produzem ataques mais sofisticados e geralmente direcionados

Possuem uma vasta gama de recursos à disposição

QUEM SÃO?

CHINA

IRÃ

RUSSIA

COREIA DO NORTE

Fontes:
Mandiant
Crowdstrike
FireEye

OBJETIVOS

Espionagem industrial, diplomática ou militar

Destruição (Wiper malware)

Ganho financeiro

TÉCNICAS

Spear phishing

Engenharia Social

Ataques em vulnerabilidades não corrigidas (unpatched vulnerabilities)

CYBER GANGUES

OBJETIVOS

Ganhos financeiros

TÉCNICAS

Spear phishing

Malware-as-a-service

Ransomware-as-a-service

Venda de informações na Dark Web

Obs: Muitos tem suas bases na Russia

MITRE | ATT&CK

Matrices Tactics Techniques Data Sources Mitigations Groups Software Campaigns Resources Blog

ATT&CKcon 4.0 will be held on Oct 24-25 in McLean, VA. Click here for more details and to register.

GROUPS

Overview

admin@338

Home > Groups

Groups

Groups are activity clusters that are tracked by a common name in the security community. Analysts track these clusters using various analytic methodologies and terms such as threat groups, activity groups, and threat actors. Some groups have multiple names associated with similar activities due to various organizations tracking similar activities by different names. Organizations' group definitions may partially overlap with groups designated by other organizations and may disagree on specific activity.

For the purposes of the Group pages, the MITRE ATT&CK team uses the term Group to refer to any of the above designations for an adversary activity cluster. The team makes a best effort to track overlaps between names based on publicly reported associations, which are designated as "Associated Groups" on each page (formerly labeled "Aliases"), because we believe these overlaps are useful for analyst awareness. We do not represent these names as exact overlaps and encourage analysts to do additional research.

Groups are mapped to publicly reported technique use and original references are included. The information provided does not represent all possible technique use by Groups, but rather a subset that is available solely through open source reporting. Groups are also mapped to reported Software used and attributed Campaigns, and related techniques for each are tracked separately on their respective pages.

Groups: 138

ID	Name	Associated Groups	Description
G0018	admin@338		admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors.
G0130	Ajax Security Team	Operation Woolen-Goldfish, AjaxTM, Rocket Kitten, Flying Kitten, Operation Saffron Rose	Ajax Security Team is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 Ajax Security Team transitioned from website defacement operations to malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies.

Mandiant is now part of Google Cloud. Learn More.

MANDIANT NOW PART OF Google Cloud

Platform Solutions Intelligence Services Resources Company

INSIGHT

Advanced Persistent Threats (APTs)

25 MIN READ

#ADVANCED PERSISTENT THREATS (APTS) #THREAT ACTORS

APT39

Suspected attribution: Iran

Target sectors: While APT39's targeting scope is global, its activities are concentra
Middle East. APT39 has prioritized the telecommunications sector, with additional
the travel industry and IT firms that support it and the high-tech industry.

Overview: The group's focus on the telecommunications and travel industries sugg
perform monitoring, tracking, or surveillance operations against specific individua
proprietary or customer data for commercial or operational purposes that serve st
requirements related to national priorities, or create additional accesses and vect
facilitate future campaigns. Government entities targeting suggests a potential se
intent to collect geopolitical data that may benefit nation-state decision making.

Associated malware: The group primarily leverages the SEAWEED and CACHEMON
along with a specific variant of the POWBAT backdoor.

Featured Cloud-Conscious Adversaries

Scattered Spider

Cozy Bear

Cosmic Wolf

Labyrinth Chollima

Nome	TTP (Tactics, Techniques and Procedures)	Casos notáveis
Comment Panda (AKA APT1, Comment Crew)	Spear phishing com hiperlinks maliciosos, backdoors customizados	APT1 roubou sistematicamente centenas de terabytes de dados de pelo menos 141 organizações e demonstrou capacidade e intenção de roubar de dezenas de organizações simultaneamente. Foca em atacar organizações em uma ampla gama de indústrias em países de língua inglesa. O tamanho da infraestrutura da APT1 sugere uma grande organização com pelo menos dezenas, mas potencialmente centenas de operadores humanos. Mandiant produziu extenso relatório reportando as atividades do grupo desde 2006
Static Kitten (AKA MuddyWater, Seedworm)	Spear phishing com anexos imitando arquivos legítimos (excel e pdf)	Novembro de 2021 lançaram uma campanha visando entidades do governo turco Ministérios da saúde e do interior, conselho tecnológico turco. Alerta emitidos pelo FBI, CISA, e governos do Reino Unido e Australia, informando que o grupo estava utilizando vulnerabilidades no Fortinet e ProxyShell visando organizações de infraestrutura, transporte e saúde pública dos EUA
Cozy Bear (AKA APT29, SolarStorm, The Dukes)	Spear phishing utilizando arquivos de um email já comprometido	Utilizaram email de uma conta comprometida de um país da OTAN para enviar emails com anexos maliciosos aos embaixadores do Brasil e de Portugal, fazendo se passar por um convite para reunião
Redeemer Ransomware builder	Ransomware-as-a-service	Promovem uma ferramenta em que você pode criar seu próprio ransomware attack customizável Caso seja bem sucedido a própria ferramenta ja cobra uma comissão de 20%

O QUE FAZER?

Phishing

Engenharia Social

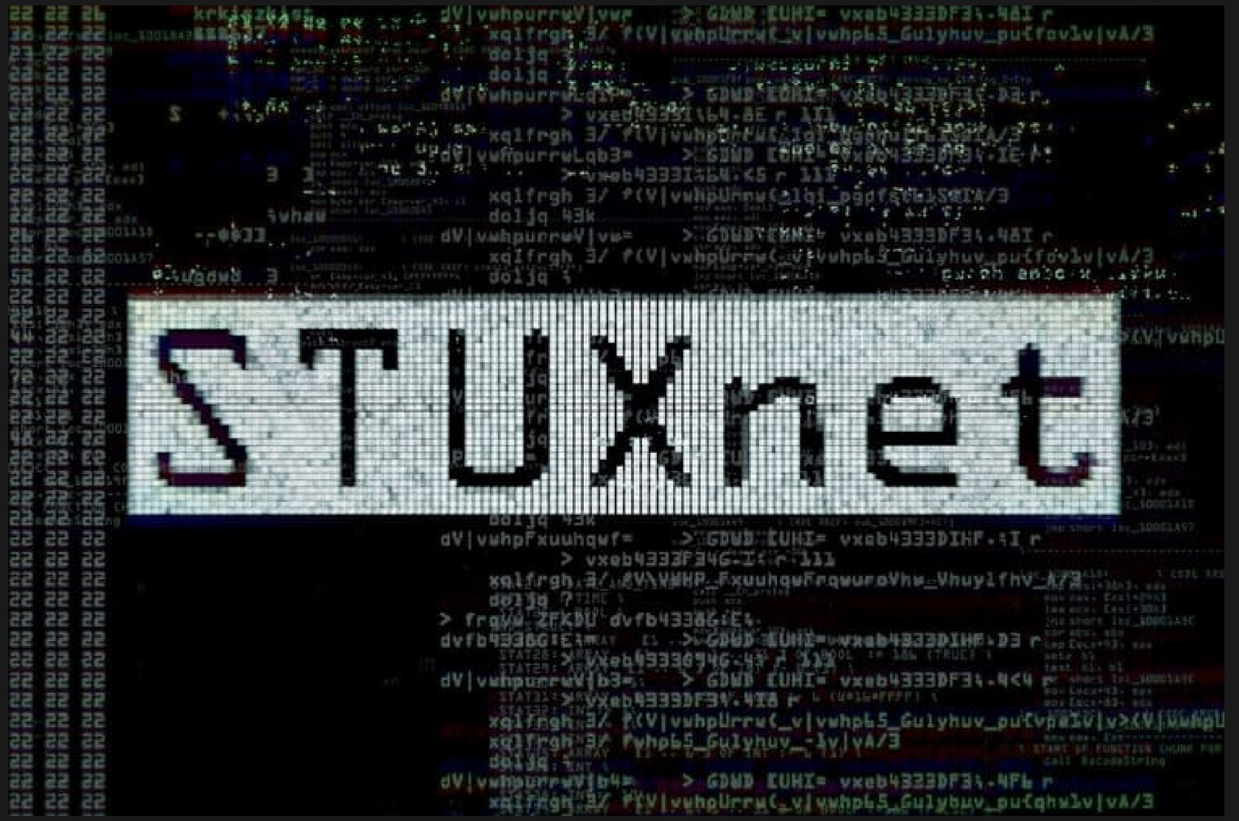
Password praying/Força Bruta

Vulnerabilidades (CVE)

Backup

EDR

Não pagar o resgate


STUXnet