Analysis of MITRE ATT&CK Groups

Scattered Spider & APT29

Prepared by:
Amer Ashoush 221006722
Omar Hamdy 221006553

Presented to:
Dr. Ehab Aboseif

What Is MITRE ATT&CK?

- Global framework for cyber adversary behavior
- Maps tactics, techniques, procedures
- Helps improve detection & defense

Why These Two Groups?

Both high-impact and active

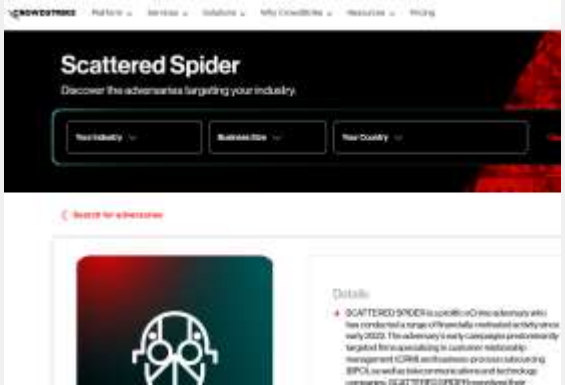
Very different motives

Ransomware vs Espionage

Strong real-world case studies

Scattered Spider Overview

- Financially motivated
- Aggressive social engineering
- Targets telecom, gaming, retail
- Ends with ransomware extortion



BlackCat Ransomware

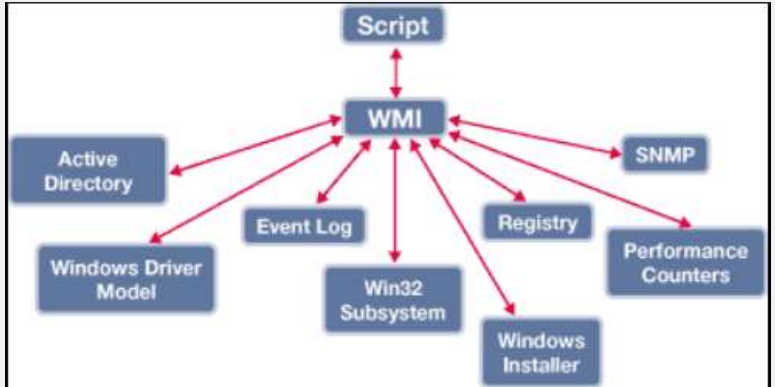
Rust-based, fast, multi-platform

Used by Scattered Spider

Encrypts systems & wipes recovery data

Technique T1047: WMI Abuse

- Uses wmic.exe to delete backups
- Blends with admin activity
- Prepares system for encryption



Technique T1047 (WMI Abuse) – Mitigations

Audit WMI activity

Enable WMI logging and monitor for suspicious commands.

Restrict WMI access

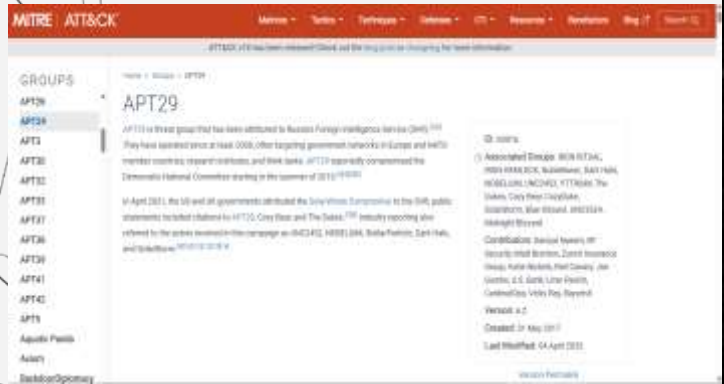
Disable remote WMI when not needed and enforce least-privilege access.

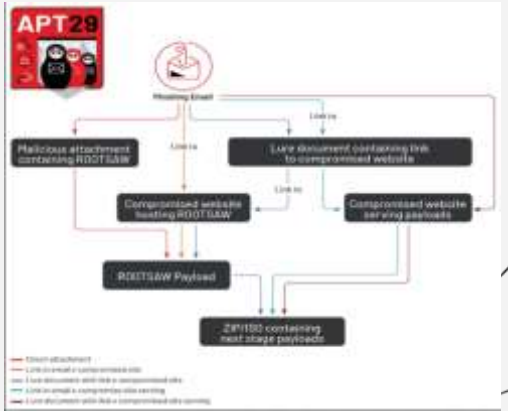
Privileged Account Controls

Use MFA, JIT (just-in-time) admin access, and rotate high-privilege credentials.

APT29 Overview

- Russian state-sponsored espionage group
- Also known as: Cozy Bear, Midnight Blizzard, Nobelium, The Dukes
- Operated by the Russian SVR (foreign intelligence service)
- Highly stealthy and persistent
- Targets government, diplomatic, research, and critical infrastructure sectors
- Heavy use of “Living off the Land” techniques (PowerShell, WMI, native tools)





Selected Software — SUNBURST (Solorigate)

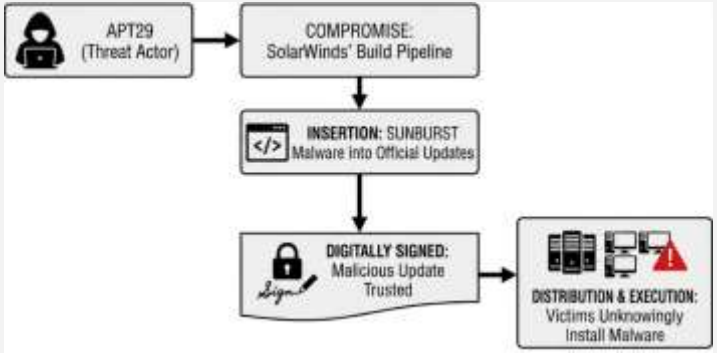
Backdoor embedded inside SolarWinds Orion updates

Delivered via a legitimate, digitally signed software update

Used to compromise U.S. government agencies & global enterprises

Technique T1195.002 — Compromise Software Supply Chain

- APT29 compromised SolarWinds' **build pipeline**
- Inserted SUNBURST into official updates
- Update was digitally signed → trusted by victims
- Victims unknowingly installed malware



Mitigations for Supply Chain Compromise

Software Integrity Controls

Validate update integrity, verify unexpected changes, continuous monitoring

Vendor / Supplier Validation

Require secure development practices, audits, transparency from vendors

Network Segmentation

Isolate systems running third-party critical software

Code Signing Policy

Require secure development practices, audits, transparency from vendors

Thank ***You !***