A faint, stylized spider web pattern serves as the background for the entire slide.

# 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

The screenshot shows the America's Cyber Defense Agency (ACDA) homepage. At the top is the ACDA logo and the text "America's Cyber Defense Agency" and "NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE". Below the logo is a navigation bar with links for "Topics", "Spotlight", "Resources & Tools", "News & Events", "Careers", and "About". Under "Topics", the "Cybersecurity Advisory" section is selected, showing a sub-menu with "Home", "New & Events", "Cybersecurity Advisory", and "Scattered Spider". The main content area features a large blue header "CYBERSECURITY ADVISORY" and the title "Scattered Spider". Below the title is the text "Last Revised: July 29, 2023" and "Alert Code: AA23-T0201". At the bottom is a "CISA PRODUCT PERFORMANCE SURVEY" button.

The screenshot shows a CrowdStrike blog post titled "Scattered Spider". The header includes the CrowdStrike logo and the word "BLOG". Below the header is a search bar with the placeholder "Search for #scatteredspider". The main content area has a heading "Scattered Spider" and the sub-heading "Discover the adversaries targeting your industry." Below this are three buttons: "Industry", "Business", and "Your Country". The main text discusses the campaign's targeting of the gaming, telecom, and retail industries, mentioning its use of spear-phishing and social engineering to exploit Windows security vulnerabilities. It also notes that the campaign is part of a broader trend of "Bring-Your-Own-Vulnerable-Driver" tactics.



The screenshot shows another CrowdStrike blog post titled "SCATTERED SPIDER Exploits Windows Security Deficiencies with Bring-Your-Own-Vulnerable-Driver Tactic in Attempt to Bypass Endpoint Security". The post features a large red and black graphic of a hooded figure with a mask, holding a device, set against a dark background with glowing red lines. The text discusses the specific exploit used by the Scattered Spider campaign to bypass endpoint security measures.

# BlackCat Ransomware



*Rust-based, fast, multi-platform*

---

*Used by Scattered Spider*

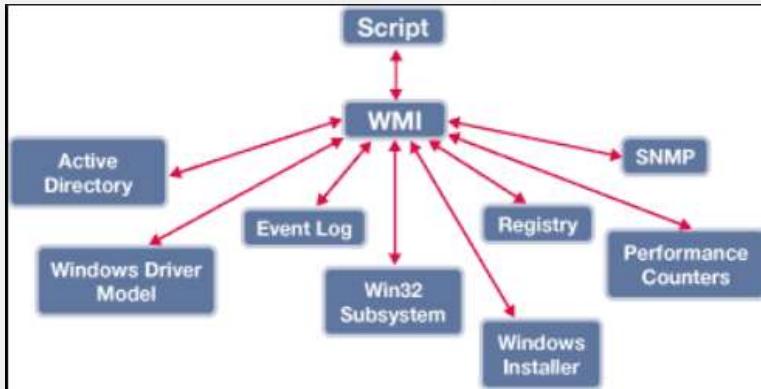
---

*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)

MITRE ATT&CK

Metrics | Teams | Techniques | Detectors | CTI | Persistence | Remediation | Kill Chain | Search | Help

Groups

More in Groups > APT29

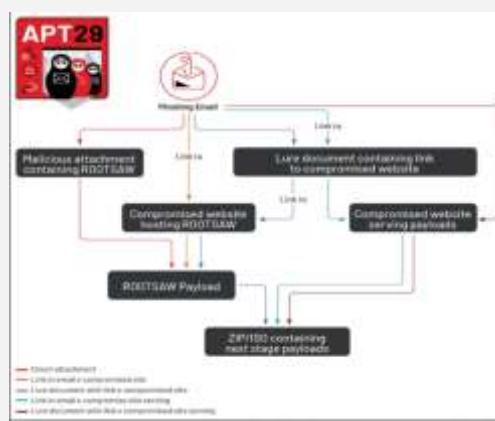
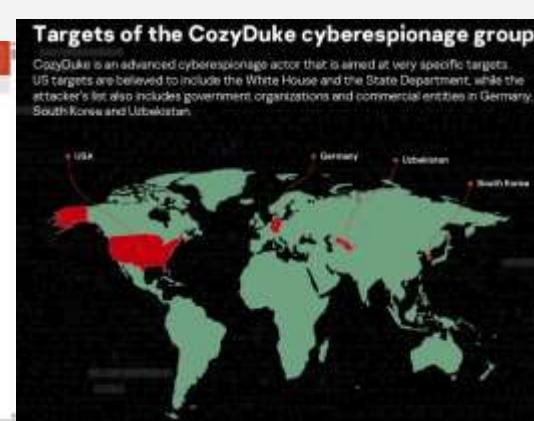
**APT29**

APT29 is a threat group that has been attributed to Russia's Foreign Intelligence Service (SVR). They have been active at least since 2008, often targeting government networks in Europe and North America, research institutions, and think tanks. APT29 reportedly compromised the Democratic National Committee during the summer of 2016 [100].

On April 2013, the US and UK governments attributed the Sony Pictures Computer Emergency Response Team (CERT) public statement included a reference to APT29, Cozy Bear, and The Dukes.<sup>[101]</sup> Industry reporting also referred to the actors involved with the campaign as BEACON, NOBEL, BANE, Stellaris, Dark Hotel, and Shadow [102-104].

Groups

- APT29
- APT28
- APT3
- APT20
- APT32
- APT33
- APT34
- APT35
- APT36
- APT37
- APT38
- APT40
- APT41
- APT42
- APT43
- APT44
- APT45
- APT46
- APT47
- APT48
- APT49
- APT50
- APT51
- APT52
- APT53
- APT54
- APT55
- APT56
- APT57
- APT58
- APT59
- APT60
- APT61
- APT62
- APT63
- APT64
- APT65
- APT66
- APT67
- APT68
- APT69
- APT70
- APT71
- APT72
- APT73
- APT74
- APT75
- APT76
- APT77
- APT78
- APT79
- APT80
- APT81
- APT82
- APT83
- APT84
- APT85
- APT86
- APT87
- APT88
- APT89
- APT90
- APT91
- APT92
- APT93
- APT94
- APT95
- APT96
- APT97
- APT98
- APT99
- APT100
- APT101
- APT102
- APT103
- APT104
- APT105
- APT106
- APT107
- APT108
- APT109
- APT110
- APT111
- APT112
- APT113
- APT114
- APT115
- APT116
- APT117
- APT118
- APT119
- APT120
- APT121
- APT122
- APT123
- APT124
- APT125
- APT126
- APT127
- APT128
- APT129
- APT130
- APT131
- APT132
- APT133
- APT134
- APT135
- APT136
- APT137
- APT138
- APT139
- APT140
- APT141
- APT142
- APT143
- APT144
- APT145
- APT146
- APT147
- APT148
- APT149
- APT150
- APT151
- APT152
- APT153
- APT154
- APT155
- APT156
- APT157
- APT158
- APT159
- APT160
- APT161
- APT162
- APT163
- APT164
- APT165
- APT166
- APT167
- APT168
- APT169
- APT170
- APT171
- APT172
- APT173
- APT174
- APT175
- APT176
- APT177
- APT178
- APT179
- APT180
- APT181
- APT182
- APT183
- APT184
- APT185
- APT186
- APT187
- APT188
- APT189
- APT190
- APT191
- APT192
- APT193
- APT194
- APT195
- APT196
- APT197
- APT198
- APT199
- APT200
- APT201
- APT202
- APT203
- APT204
- APT205
- APT206
- APT207
- APT208
- APT209
- APT210
- APT211
- APT212
- APT213
- APT214
- APT215
- APT216
- APT217
- APT218
- APT219
- APT220
- APT221
- APT222
- APT223
- APT224
- APT225
- APT226
- APT227
- APT228
- APT229
- APT230
- APT231
- APT232
- APT233
- APT234
- APT235
- APT236
- APT237
- APT238
- APT239
- APT240
- APT241
- APT242
- APT243
- APT244
- APT245
- APT246
- APT247
- APT248
- APT249
- APT250
- APT251
- APT252
- APT253
- APT254
- APT255
- APT256
- APT257
- APT258
- APT259
- APT260
- APT261
- APT262
- APT263
- APT264
- APT265
- APT266
- APT267
- APT268
- APT269
- APT270
- APT271
- APT272
- APT273
- APT274
- APT275
- APT276
- APT277
- APT278
- APT279
- APT280
- APT281
- APT282
- APT283
- APT284
- APT285
- APT286
- APT287
- APT288
- APT289
- APT290
- APT291
- APT292
- APT293
- APT294
- APT295
- APT296
- APT297
- APT298
- APT299
- APT300
- APT301
- APT302
- APT303
- APT304
- APT305
- APT306
- APT307
- APT308
- APT309
- APT310
- APT311
- APT312
- APT313
- APT314
- APT315
- APT316
- APT317
- APT318
- APT319
- APT320
- APT321
- APT322
- APT323
- APT324
- APT325
- APT326
- APT327
- APT328
- APT329
- APT330
- APT331
- APT332
- APT333
- APT334
- APT335
- APT336
- APT337
- APT338
- APT339
- APT340
- APT341
- APT342
- APT343
- APT344
- APT345
- APT346
- APT347
- APT348
- APT349
- APT350
- APT351
- APT352
- APT353
- APT354
- APT355
- APT356
- APT357
- APT358
- APT359
- APT360
- APT361
- APT362
- APT363
- APT364
- APT365
- APT366
- APT367
- APT368
- APT369
- APT370
- APT371
- APT372
- APT373
- APT374
- APT375
- APT376
- APT377
- APT378
- APT379
- APT380
- APT381
- APT382
- APT383
- APT384
- APT385
- APT386
- APT387
- APT388
- APT389
- APT390
- APT391
- APT392
- APT393
- APT394
- APT395
- APT396
- APT397
- APT398
- APT399
- APT400
- APT401
- APT402
- APT403
- APT404
- APT405
- APT406
- APT407
- APT408
- APT409
- APT410
- APT411
- APT412
- APT413
- APT414
- APT415
- APT416
- APT417
- APT418
- APT419
- APT420
- APT421
- APT422
- APT423
- APT424
- APT425
- APT426
- APT427
- APT428
- APT429
- APT430
- APT431
- APT432
- APT433
- APT434
- APT435
- APT436
- APT437
- APT438
- APT439
- APT440
- APT441
- APT442
- APT443
- APT444
- APT445
- APT446
- APT447
- APT448
- APT449
- APT450
- APT451
- APT452
- APT453
- APT454
- APT455
- APT456
- APT457
- APT458
- APT459
- APT460
- APT461
- APT462
- APT463
- APT464
- APT465
- APT466
- APT467
- APT468
- APT469
- APT470
- APT471
- APT472
- APT473
- APT474
- APT475
- APT476
- APT477
- APT478
- APT479
- APT480
- APT481
- APT482
- APT483
- APT484
- APT485
- APT486
- APT487
- APT488
- APT489
- APT490
- APT491
- APT492
- APT493
- APT494
- APT495
- APT496
- APT497
- APT498
- APT499
- APT500
- APT501
- APT502
- APT503
- APT504
- APT505
- APT506
- APT507
- APT508
- APT509
- APT510
- APT511
- APT512
- APT513
- APT514
- APT515
- APT516
- APT517
- APT518
- APT519
- APT520
- APT521
- APT522
- APT523
- APT524
- APT525
- APT526
- APT527
- APT528
- APT529
- APT530
- APT531
- APT532
- APT533
- APT534
- APT535
- APT536
- APT537
- APT538
- APT539
- APT540
- APT541
- APT542
- APT543
- APT544
- APT545
- APT546
- APT547
- APT548
- APT549
- APT550
- APT551
- APT552
- APT553
- APT554
- APT555
- APT556
- APT557
- APT558
- APT559
- APT560
- APT561
- APT562
- APT563
- APT564
- APT565
- APT566
- APT567
- APT568
- APT569
- APT570
- APT571
- APT572
- APT573
- APT574
- APT575
- APT576
- APT577
- APT578
- APT579
- APT580
- APT581
- APT582
- APT583
- APT584
- APT585
- APT586
- APT587
- APT588
- APT589
- APT590
- APT591
- APT592
- APT593
- APT594
- APT595
- APT596
- APT597
- APT598
- APT599
- APT600
- APT601
- APT602
- APT603
- APT604
- APT605
- APT606
- APT607
- APT608
- APT609
- APT610
- APT611
- APT612
- APT613
- APT614
- APT615
- APT616
- APT617
- APT618
- APT619
- APT620
- APT621
- APT622
- APT623
- APT624
- APT625
- APT626
- APT627
- APT628
- APT629
- APT630
- APT631
- APT632
- APT633
- APT634
- APT635
- APT636
- APT637
- APT638
- APT639
- APT640
- APT641
- APT642
- APT643
- APT644
- APT645
- APT646
- APT647
- APT648
- APT649
- APT650
- APT651
- APT652
- APT653
- APT654
- APT655
- APT656
- APT657
- APT658
- APT659
- APT660
- APT661
- APT662
- APT663
- APT664
- APT665
- APT666
- APT667
- APT668
- APT669
- APT670
- APT671
- APT672
- APT673
- APT674
- APT675
- APT676
- APT677
- APT678
- APT679
- APT680
- APT681
- APT682
- APT683
- APT684
- APT685
- APT686
- APT687
- APT688
- APT689
- APT690
- APT691
- APT692
- APT693
- APT694
- APT695
- APT696
- APT697
- APT698
- APT699
- APT700
- APT701
- APT702
- APT703
- APT704
- APT705
- APT706
- APT707
- APT708
- APT709
- APT710
- APT711
- APT712
- APT713
- APT714
- APT715
- APT716
- APT717
- APT718
- APT719
- APT720
- APT721
- APT722
- APT723
- APT724
- APT725
- APT726
- APT727
- APT728
- APT729
- APT730
- APT731
- APT732
- APT733
- APT734
- APT735
- APT736
- APT737
- APT738
- APT739
- APT740
- APT741
- APT742
- APT743
- APT744
- APT745
- APT746
- APT747
- APT748
- APT749
- APT750
- APT751
- APT752
- APT753
- APT754
- APT755
- APT756
- APT757
- APT758
- APT759
- APT760
- APT761
- APT762
- APT763
- APT764
- APT765
- APT766
- APT767
- APT768
- APT769
- APT770
- APT771
- APT772
- APT773
- APT774
- APT775
- APT776
- APT777
- APT778
- APT779
- APT780
- APT781
- APT782
- APT783
- APT784
- APT785
- APT786
- APT787
- APT788
- APT789
- APT790
- APT791
- APT792
- APT793
- APT794
- APT795
- APT796
- APT797
- APT798
- APT799
- APT800
- APT801
- APT802
- APT803
- APT804
- APT805
- APT806
- APT807
- APT808
- APT809
- APT810
- APT811
- APT812
- APT813
- APT814
- APT815
- APT816
- APT817
- APT818
- APT819
- APT820
- APT821
- APT822
- APT823
- APT824
- APT825
- APT826
- APT827
- APT828
- APT829
- APT830
- APT831
- APT832
- APT833
- APT834
- APT835
- APT836
- APT837
- APT838
- APT839
- APT840
- APT841
- APT842
- APT843
- APT844
- APT845
- APT846
- APT847
- APT848
- APT849
- APT850
- APT851
- APT852
- APT853
- APT854
- APT855
- APT856
- APT857
- APT858
- APT859
- APT860
- APT861
- APT862
- APT863
- APT864
- APT865
- APT866
- APT867
- APT868
- APT869
- APT870
- APT871
- APT872
- APT873
- APT874
- APT875
- APT876
- APT877
- APT878
- APT879
- APT880
- APT881
- APT882
- APT883
- APT884
- APT885
- APT886
- APT887
- APT888
- APT889
- APT890
- APT891
- APT892
- APT893
- APT894
- APT895
- APT896
- APT897
- APT898
- APT899
- APT900
- APT901
- APT902
- APT903
- APT904
- APT905
- APT906
- APT907
- APT908
- APT909
- APT910
- APT911
- APT912
- APT913
- APT914
- APT915
- APT916
- APT917
- APT918
- APT919
- APT920
- APT921
- APT922
- APT923
- APT924
- APT925
- APT926
- APT927
- APT928
- APT929
- APT930
- APT931
- APT932
- APT933
- APT934
- APT935
- APT936
- APT937
- APT938
- APT939
- APT940
- APT941
- APT942
- APT943
- APT944
- APT945
- APT946
- APT947
- APT948
- APT949
- APT950
- APT951
- APT952
- APT953
- APT954
- APT955
- APT956
- APT957
- APT958
- APT959
- APT960
- APT961
- APT962
- APT963
- APT964
- APT965
- APT966
- APT967
- APT968
- APT969
- APT970
- APT971
- APT972
- APT973
- APT974
- APT975
- APT976
- APT977
- APT978
- APT979
- APT980
- APT981
- APT982
- APT983
- APT984
- APT985
- APT986
- APT987
- APT988
- APT989
- APT990
- APT991
- APT992
- APT993
- APT994
- APT995
- APT996
- APT997
- APT998
- APT999
- APT1000



# Selected Software — SUNBURST (Solarigate)

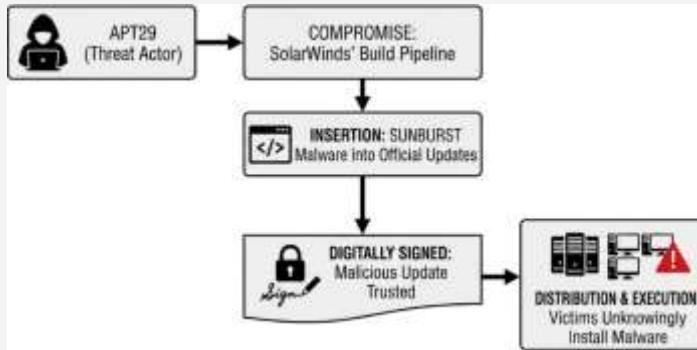


*Backdoor embedded inside  
SolarWinds Orion updates*

*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 !**

---