RED SKY® ALLIANCE

TLP GREEN

INTELLIGENCE REPORT: CYBER THREATS – ALL SECTOR **SER. NO.: IR-21-300-001**

Activity Summary - Week Ending on 27 October 2021:

- ✓ Red Sky Alliance identified 36,141 connections from new IP's checking in with our Sinkholes
- ✓ Analysts identified 41,071 new IP addresses participating in various Botnets
- ✓ Sality remains the top Malware Variant at 32074 times seen
- ✓ Harvester Part II
- ✓ Vulnerability on Confluence Server
- ✓ EntroLink
- ✓ Russia, Russia, Russia
- ✓ Iranian Gas Stations
- ✓ Walmart
- ✓ COP = Climate Activism escalation
- ✓ Climate and Animal Rights Activists join Forces to eliminate Meat

COMPROMISED (C2) IP'S

IP	Contacts
134.209.127.243	83
176.122.25.12	76
185.41.152.102	75
91.188.215.198	70
213.238.178.239	59

37.0.11.64 – was found in IPAbuse database. This IP was reported 126 times. Confidence of Abuse is 100%: ISP: Serverion BV; Usage Type: Data Center/Web Hosting/Transit; Domain Name: legaconetworks.nl; Country: Netherlands; City: Brielle, Zuid-Holland
https://www.abuseipdb.com/check/37.0.11.64

On 26 October 2021, Red Sky Alliance identified **36,141** connections from new unique IP addresses, which are checking in with one of the many Red Sky Alliance sinkholed domains.

MALWARE ACTIVITY

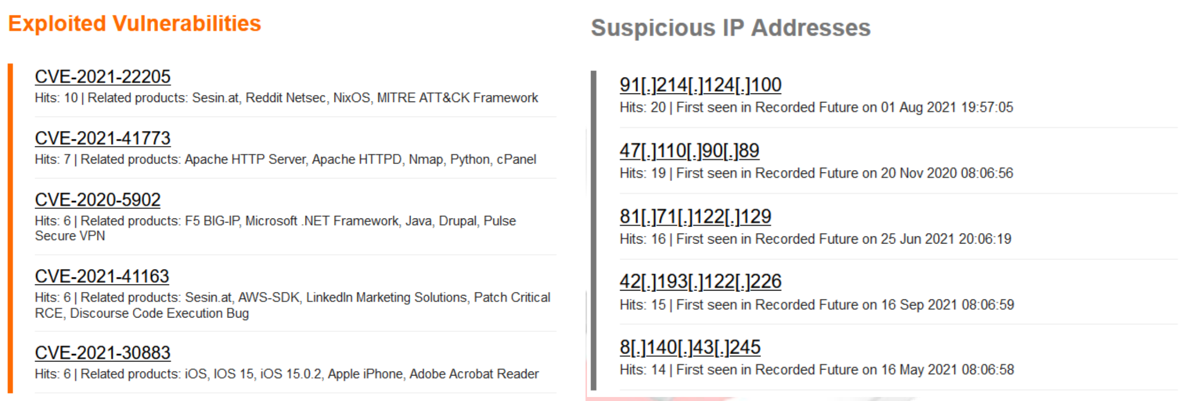
Malware Variant	Times Seen
sality	32074
corkow	2298
sykipot	635
betabot	442
shiz	315

Top 5 Malware Variant and number of contacts. Sality and Corkow has consistently remain the top variants. Skipot is next.

For a full list – contact analysts: info@wapacklabs.com

On 26 October 2021, analysts identified **41,071** new IP addresses participating in various botnets (call for full .csv Blacklists, below are only a small sampling of botnet trackers)

First_ Seen	Botnet Attribution	Infected Host's IPv4 Address
2021-10-17T07:20:39	SOCKS4 proxy|port:4145	1.0.145.246
2021-10-21T20:52:37	HTTP proxy|port:8080	1.0.212.144
2021-10-21T15:01:26	HTTP proxy|port:80	1.1.1.237
2021-10-21T13:03:37	HTTP proxy|port:80	1.1.1.240
2021-10-21T14:42:38	HTTP proxy|port:80	1.1.1.242



Exploited Vulnerabilities

CVE-2021-22205
Hits: 10 | Related products: Sesin.at, Reddit Netsec, NixOS, MITRE ATT&CK Framework

CVE-2021-41773
Hits: 7 | Related products: Apache HTTP Server, Apache HTTPD, Nmap, Python, cPanel

CVE-2020-5902
Hits: 6 | Related products: F5 BIG-IP, Microsoft .NET Framework, Java, Drupal, Pulse Secure VPN

CVE-2021-41163
Hits: 6 | Related products: Sesin.at, AWS-SDK, LinkedIn Marketing Solutions, Patch Critical RCE, Discourse Code Execution Bug

CVE-2021-30883
Hits: 6 | Related products: iOS, IOS 15, iOS 15.0.2, Apple iPhone, Adobe Acrobat Reader

Suspicious IP Addresses

91[.]214[.]124[.]100
Hits: 20 | First seen in Recorded Future on 01 Aug 2021 19:57:05

47[.]110[.]90[.]89
Hits: 19 | First seen in Recorded Future on 20 Nov 2020 08:06:56

81[.]71[.]122[.]129
Hits: 16 | First seen in Recorded Future on 25 Jun 2021 20:06:19

42[.]193[.]122[.]226
Hits: 15 | First seen in Recorded Future on 16 Sep 2021 08:06:59

8[.]140[.]43[.]245
Hits: 14 | First seen in Recorded Future on 16 May 2021 08:06:58

Recorded Future Top 5 Threat Actors and Malware for 10 27 2021 (rankings change daily)

MALICIOUS CYBER TRENDS [1]

Rank Name		%
1	W32/VBNA.HLT!worm	21
2	W32/GenKryptik.DPIE!tr	21
3	W32/Dropper.DT!tr	20
4	JS/RefC.G!tr	19
5	W32/Agent.BMGF!tr.dldr	19

New Threat Actor **Harvester** Focuses on South Asian Targets with New Cyber Weapons – Researchers are aware of a report that a new threat actor, "Harvester," attacked targets in South Asia with previously unseen weapons for cyber espionage. Symantec reports the Harvester group began its activities in June 2021 and targeted telecommunications, government, and information technology (IT) organizations in the region with a special focus on Afghanistan. Researchers believe that Harvester is a nation-state-backed threat actor. While the initial infection vector has not been identified, activities involving a URL were found on the victim's machine from which a custom backdoor, downloader and screenshotter were likely deployed. Also, Cobalt Strike and Metasploit were reportedly found on the compromised system. The custom backdoor communicates with the attacker's Command and Control (C&C) servers, where stolen data was encrypted and sent to. The custom

[1] Fortinet Intel, 10 15 2021

downloader installs a DLL, creates a loadpoint, and opens an embedded web browser within its own UI. The custom screenshotter takes screenshots and saves them to a password-protected zip file as part of information-stealing activities. Link to full report: https://www.fortiguard.com/threat-signal-report/4204/new-threat-actor-harvester-focuses-on-south-asian-targets-with-new-cyber-weapons

Signatures: MSIL/Agent.UWS!tr PossibleThreat.PALLAS.H W64/Cobalt.LXTDIKT!tr VBS/Starter.BC42!tr MSIL/BackDoor.3CD3!tr

Indicator(s):

- 0740cc87a7d028ad45a3d54540b91c4d90b6fc54d83bb01842cf23348b25bc42
- 3c34c23aef8934651937c31be7420d2fc8a22ca260f5afdda0f08f4d3730ae59
- 470cd1645d1da5566eef36c6e0b2a8ed510383657c4030180eb0083358813cd3
- 691e170c5e42dd7d488b9d47396b633a981640f8ab890032246bf37704d4d865
- c4b6d7e88a63945f3e0768657e299d2d3a4087266b4fc6b1498e2435e311f5d1

Recent Attack Uses **Vulnerability on Confluence Server** – Back in August 2021, Atlassian published a security advisory about the CVE-2021-26084 vulnerability that could enable a threat actor to run arbitrary code on unpatched Confluence Server and Data Center instances. At that time, researchers analyzed the situation and published the relevant information showing massive scanning for the vulnerability was observed and proof-of-concept exploit code was seen in public. FortiGuard Labs has followed up with a blog that analyzes the payloads leveraging this vulnerability, takes a deep dive into the attack and provides related IOCs so organizations can check their network to see if they have been affected by CVE-2021-26084. Full details seen here: https://www.fortinet.com/blog/threat-research/recent-attack-uses-vulnerability-on-confluence-server

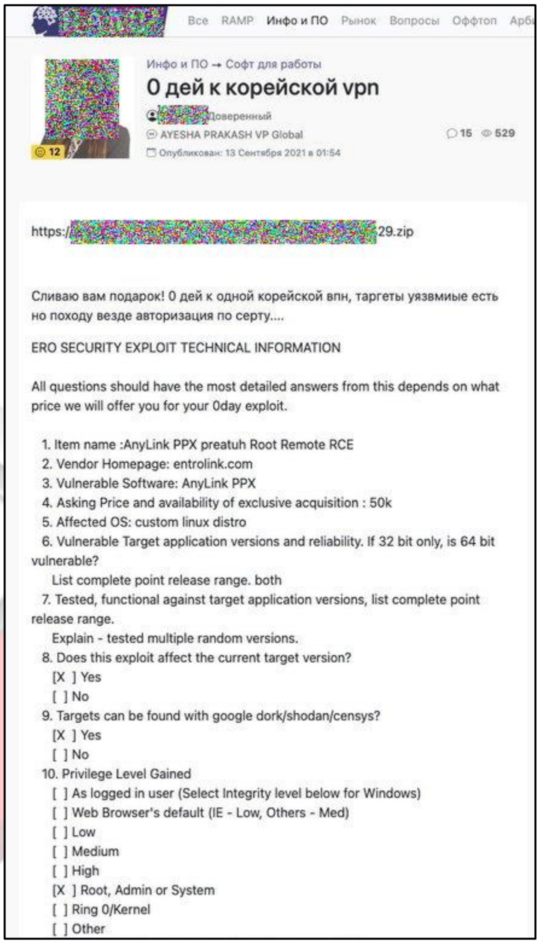
Indicator(s):

- 86(.)105(.)195(.)120
- 86(.)105(.)195(.)154
- 149(.)28(.)85(.)17
- 2(.)57(.)33(.)59
- 141(.)98(.)83(.)139
- 98(.)239(.)93(.)20
- 87(.)106(.)194(.)46
- 51(.)75(.)195(.)137
- 34(.)247(.)148(.)227
- 121(.)196(.)25(.)170
- 221(.)168(.)37(.)77
- 122(.)9(.)48(.)250
- 18(.)182(.)153(.)49
- 209(.)141(.)50(.)210

GLOBAL TRENDS:

EntroLink - Multiple ransomware gangs have weaponized and are abusing a zero-day in EntroLink VPN appliances after an exploit was released on an underground cybercrime forum at the start of September 2021. The zero-day is believed to impact EntroLink PPX-AnyLink devices, popular with South Korean companies, and used as user authentication gateways and VPNs to allow employees remote access to company networks and internal resources. An exploit targeting these devices was released last month, on 13 September 2021.[2]

The exploit, initially sold on another forum for $50,000, was released for free by the administrator of a newly-launched cybercrime forum in what appears to be a promotional stunt meant to raise the site's profile among other cybercrime groups.



Инфо и ПО → Софт для работы

0 дей к корейской vpn

[redacted] Доверенный

AYESHA PRAKASH VP Global

Опубликован: 13 Сентября 2021 в 01:54

12　15　529

https:/[redacted]29.zip

Сливаю вам подарок! 0 дей к одной корейской впн, таргеты уязвмиые есть но походу везде авторизация по серту....

ERO SECURITY EXPLOIT TECHNICAL INFORMATION

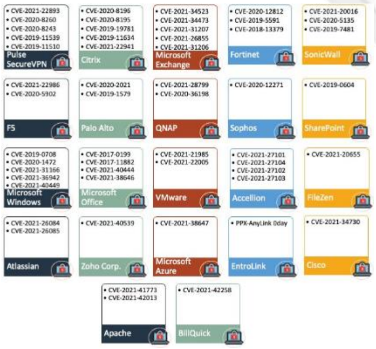
All questions should have the most detailed answers from this depends on what price we will offer you for your 0day exploit.

1. Item name :AnyLink PPX preatuh Root Remote RCE
2. Vendor Homepage: entrolink.com
3. Vulnerable Software: AnyLink PPX
4. Asking Price and availability of exclusive acquisition : 50k
5. Affected OS: custom linux distro
6. Vulnerable Target application versions and reliability. If 32 bit only, is 64 bit vulnerable?
   List complete point release range. both
7. Tested, functional against target application versions, list complete point release range.
   Explain - tested multiple random versions.
8. Does this exploit affect the current target version?
   [X] Yes
   [ ] No
9. Targets can be found with google dork/shodan/censys?
   [X] Yes
   [ ] No
10. Privilege Level Gained
   [ ] As logged in user (Select Integrity level below for Windows)
   [ ] Web Browser's default (IE - Low, Others - Med)
   [ ] Low
   [ ] Medium
   [ ] High
   [X] Root, Admin or System
   [ ] Ring 0/Kernel
   [ ] Other

According to the forum post, the exploit is still unpatched, exploits a network protocol, and grants remote code execution with root-level access to PPX-AnyLink devices. The post also describes the bug as an input validation issue and that the exploit is self-contained and only needs a few seconds to compromise a device.

Since the exploit's release, affiliates for the BlackMatter and LockBit ransomware operations have been linked to possible intrusions where this exploit might have been used, according to a researcher who is currently tracking and investigating ransomware attacks.

EntroLink, the South Korean networking vendor, was notified of the exploit's release by the security researcher, yet have not responded to media inquiries.



Pulse SecureVPN
- CVE-2021-22893
- CVE-2020-8260
- CVE-2020-8243
- CVE-2019-11539
- CVE-2019-11510

Citrix
- CVE-2020-8196
- CVE-2020-8195
- CVE-2019-19781
- CVE-2019-11634
- CVE-2021-22941

Microsoft Exchange
- CVE-2021-34523
- CVE-2021-34473
- CVE-2021-31207
- CVE-2021-26855
- CVE-2021-31206

Fortinet
- CVE-2020-12812
- CVE-2019-5591
- CVE-2018-13379

SonicWall
- CVE-2021-20016
- CVE-2020-5135
- CVE-2019-7481

F5
- CVE-2021-22986
- CVE-2020-5902

Palo Alto
- CVE-2020-2021
- CVE-2019-1579

QNAP
- CVE-2021-28799
- CVE-2020-36198

Sophos
- CVE-2020-12271

SharePoint
- CVE-2019-0604

Microsoft Windows
- CVE-2019-0708
- CVE-2020-1472
- CVE-2021-31166
- CVE-2021-36942
- CVE-2021-40449

Microsoft Office
- CVE-2017-0199
- CVE-2017-11882
- CVE-2021-40444
- CVE-2021-38646

VMware
- CVE-2021-21985
- CVE-2021-22005

Accellion
- CVE-2021-27101
- CVE-2021-27104
- CVE-2021-27102
- CVE-2021-27103

FileZen
- CVE-2021-20655

Atlassian
- CVE-2021-26084
- CVE-2021-26085

Zoho Corp.
- CVE-2021-40539

Microsoft Azure
- CVE-2021-38647

EntroLink
- PPX-AnyLink 0day

Cisco
- CVE-2021-34730

Apache
- CVE-2021-41773
- CVE-2021-42013

BillQuick
- CVE-2021-42258

The EntroLink PPX-AnyLink exploit now becomes the 54th zero-day vulnerability that ransomware gangs are currently known to abuse, according to a tracker managed by security researchers Allan L. and Pancak3.

Russia, Russia, Russia - Russian-linked hackers are being blamed for the massive cyberattack on the US last year have been targeting hundreds of companies and organizations in its latest wave of attacks on US-based computer networks. This as the White House is dismissing the incident as "unsophisticated, run-of-the-mill operations." In a blog post over last weekend, Microsoft said Nobelium — the Russian-based agency behind last year's widespread SolarWinds attack — has been targeting cloud service providers and technology service organizations in a bid to obtain data.[3] The attacks have targeted organizations in the US and Europe since May, Microsoft said.

One of Microsoft's top security officers, told media sources that the latest attack was "very large and ongoing." "Nobelium has been attempting to replicate the approach it has used in past attacks by targeting organizations

[2] https://therecord.media/ransomware-gangs-are-abusing-a-zero-day-in-entrolink-vpn-appliances/

[3] https://nypost.com/2021/10/25/russian-hackers-target-us-networks-in-ongoing-cyberattack/

integral to the global IT supply chain. This time, it is attacking a different part of the supply chain: resellers and other technology service providers that customize, deploy and manage cloud services and other technologies on behalf of their customers," Microsoft said in its blog post. "We (Microsoft) believe Nobelium ultimately hopes to piggyback on any direct access that resellers may have to their customers' IT systems and more easily impersonate an organization's trusted technology partner to gain access to their downstream customers." Microsoft said it had notified 609 customers between 1 July and 19 October 2021 that they had been attacked. The company insisted only a small percentage of the latest attempts were successful.

"This recent activity is another indicator that Russia is trying to gain long-term, systematic access to a variety of points in the technology supply chain and establish a mechanism for surveilling — now or in the future — targets of interest to the Russian government," Microsoft said. "The attacks we've observed in the recent campaign against resellers and service providers have not attempted to exploit any flaw or vulnerability in software but rather used well-known techniques, like password spray and phishing, to steal legitimate credentials and gain privileged access."

Microsoft said it had learned enough about these new attacks to provide information that "can be used to defend against this new approach."   A US administration official told media the latest attacks were "unsophisticated, run-of-the-mill operations that could have been prevented if the cloud service providers had implemented baseline cybersecurity practices." "We can do a lot of things … but the responsibility to implement simple cybersecurity practices to lock their — and by extension, our — digital doors rests with the private sector," the official said.

The US government have blamed Russia for last year's the major breach of government agencies known as the SolarWinds hack. The Biden administration has not blamed Russian President Vladimir Putin for the latest cyberattacks on US-based computer networks. Ah, international politics.

Iranian Gas Stations - Gas stations across Iran malfunctioned on 26 October 2021 reportedly due to a massive cyberattack, according to Iranian state media. While the exact details of this attack are still unclear, speculation is already rife about whether the purported cyberattack came from the US, Israel or a range of local Iranian anti-regime groups. According to various media reports, messages were posted in some systems that were hacked, addressing Iran Supreme Leader Ayatollah Ali Khamenei directly and demanding to know, "Where is the gas?" The attack comes around two years after nationwide protests of gas shortages in fall 2019.[4] "The disruption at the refueling system of gas stations... in the past few hours, was caused by a cyberattack," state broadcaster IRIB said. "Technical experts are fixing the problem and soon the refueling process... will return to normal."

Iran's Oil Ministry said only sales with smart cards used for cheaper rationed gasoline were disrupted and that clients could still buy fuel at higher rates, the ministry's news agency SHANA reported. Last week, Iran carried out a complex and coordinated strike on US forces in Syria, using up to five armed drones to strike at the Tanf garrison, a key strategic point near the Jordanian and Iraqi border. The attack was the latest in a series of such drone strikes on US forces.

In a press briefing on Monday, the US Envoy to Iran referenced potential upcoming US actions to deter Iranian aggression within the region, while refusing to hint what those actions might be. The US is considered the world's

[4] https://www.jpost.com/breaking-news/iran-gas-stations-hit-by-cyber-attack-report-683141

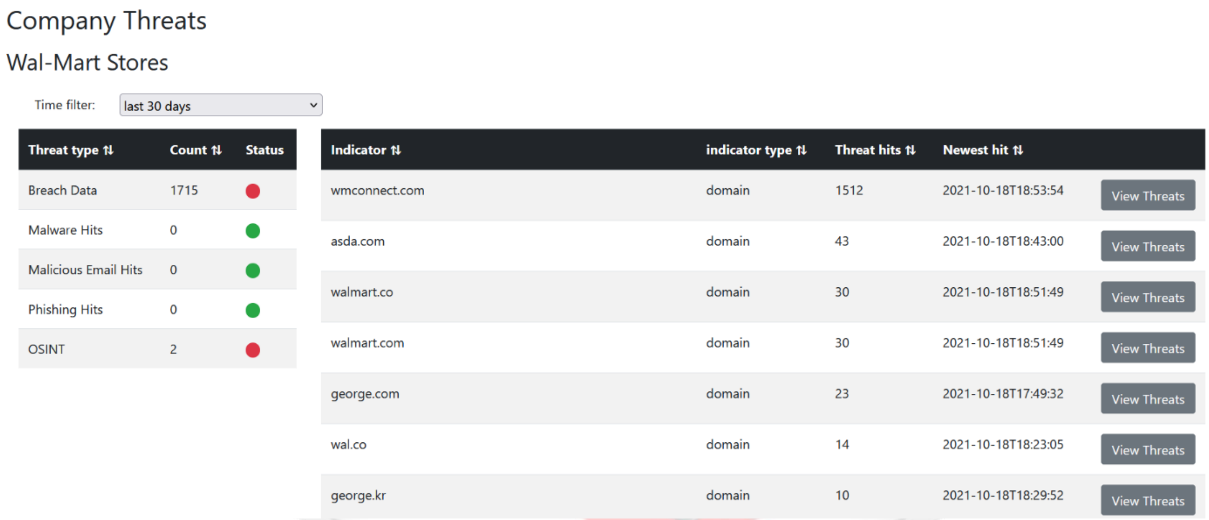
greatest offensive cyber power by far but has often been hesitant to use its offensive cyber capabilities against groups other than ISIS, for fear of a cyber retaliation. Under the previous US administration, the US did hack certain major Iranian intelligence sea-based operations to get the Islamic Republic to cease cyber attacking American allies at sea. But the current administration has not done so to date, as it has focused on building goodwill for a mutual return to the 2015 Iran nuclear deal. Israel reportedly hacked Iran's Shahid Rajaee Port on 9 May 2020, as a counter strike for an attempted Iranian cyber strike on Israel's water supply the previous month. Iran has also accused the Israeli Mossad, the US and various European intelligence agencies of using the STUXNET virus to hack its Natanz nuclear facility in 2009-2010.

A former Shin Bet (Israel Security Agency) cyber official told an Israeli radio outlet on 26 October that there was a good chance the hacker would have to be a nation-state to accomplish such a widespread hack. Yet in recent months Israel has also seen amateur hackers cause major problems to the US and European powers with sophisticated ransomware and other attacks, and the Khamenei regime has many local enemies from Iran's many minorities.

In August of this year, Check Point Software Technologies issued a report stating that an Iranian dissident group called Indra executed the mega-hack on the Islamic Republic's train system on 9 July 2021, not Israel. Check Point said Indra's hack of Iran's train system was "an example for governments around the world of how a single group can create disruption on critical infrastructure." Part of what was so unusual about the attack was that it was a non-state organization inflicting nation-state-level damage onto Iran's physical infrastructure on a nation-state level. Of non-state groups are traditionally thought of as lacking the capability to do more than hack websites and data, this was an example of such a group causing profound real-world damage.

Indra's tools destroyed data without direct means to recover it by using a "wiper," or malware designed to wipe the entire data system of critical infrastructure, making the recovery process complicated, locking users out of machines, changing passwords, and replacing wallpapers to custom messages crafted by attackers. Part of the attack included the posting of fake messages about train delays and cancellations on terminal display boards across Iran.

Dark Web Collection/Analysis
Walmart
Last 30 days / 1715 - Breach Data hits



Company Threats

Wal-Mart Stores

Time filter: last 30 days

Threat type ⇅	Count ⇅	Status
Breach Data	1715	●
Malware Hits	0	●
Malicious Email Hits	0	●
Phishing Hits	0	●
OSINT	2	●

Indicator ⇅	indicator type ⇅	Threat hits ⇅	Newest hit ⇅	
wmconnect.com	domain	1512	2021-10-18T18:53:54	View Threats
asda.com	domain	43	2021-10-18T18:43:00	View Threats
walmart.co	domain	30	2021-10-18T18:51:49	View Threats
walmart.com	domain	30	2021-10-18T18:51:49	View Threats
george.com	domain	23	2021-10-18T17:49:32	View Threats
wal.co	domain	14	2021-10-18T18:23:05	View Threats
george.kr	domain	10	2021-10-18T18:29:52	View Threats

Walmart Inc. is an American multinational retail corporation that operates a chain of hypermarkets, discount department stores, and grocery stores from the United States, headquartered in Bentonville, Arkansas. They have an enormous shupplu chain, one which is vulnerable to cyber-attacks.

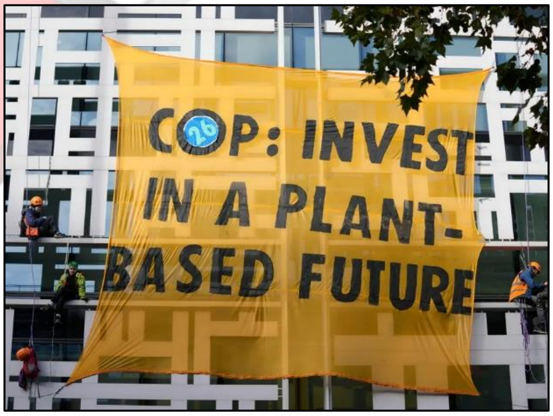
Activist Corner [5] [6]

Climate activists have begun a hunger strike outside the White House to demand US President Joe Biden take action on the climate crisis. Sunrise Movement (SM), a campaign group of young people who want to stop climate change, want Biden to pass the Build Back Better Agenda with its full range of environmental policies. SM is a youth based climate activist organization, patterned after the European group, Extinction Rebellion. The SM statement reads: "We must pass the full scope of this bill or we will spiral deeper into the climate crisis. The urgency of now cannot be understated: This could be our last chance to pass federal climate policy for the rest of the decade and we won't back down without a fight. The time is now and we have nothing to lose. No climate, no deal."

Not to be outdone, A group of climate activists tied up traffic on 25 October on a main Canadian road to Vancouver International Airport. According to Extinction Rebellion, 18-20 activists were arrested. The protest tactic seems to have worked: Extinction Rebellion Vancouver spokesperson received some airtime on CBC Radio One to explain why the group has launched a 14-day campaign of peaceful civil disobedience. Similar protests were seen in the US on NY City highways (FDR Parkway).

Climate activists in hard hats scaled a UK government building Tuesday, unfurling a banner demanding that countries attending the upcoming UN climate conference invest in plant-based alternatives to meat.

British authorities obtained a High Court injunction on Monday to stop climate change activists blockading major roads, after protesters resumed a campaign to disrupt traffic following a 10-day hiatus. The protests by Insulate Britain, a group demanding that the government provide more insulation for millions of homes, have previously brought chaos for drivers and long tailbacks, mainly on the M25 orbital motorway around the capital.



[5] https://www.kalw.org/show/your-call/2021-10-26/day-7-of-the-youth-hunger-strike-for-climate-justice-outside-the-white-house

[6] https://www.reuters.com/business/cop/climate-change-protesters-restart-campaign-with-city-london-blockades-2021-10-25/