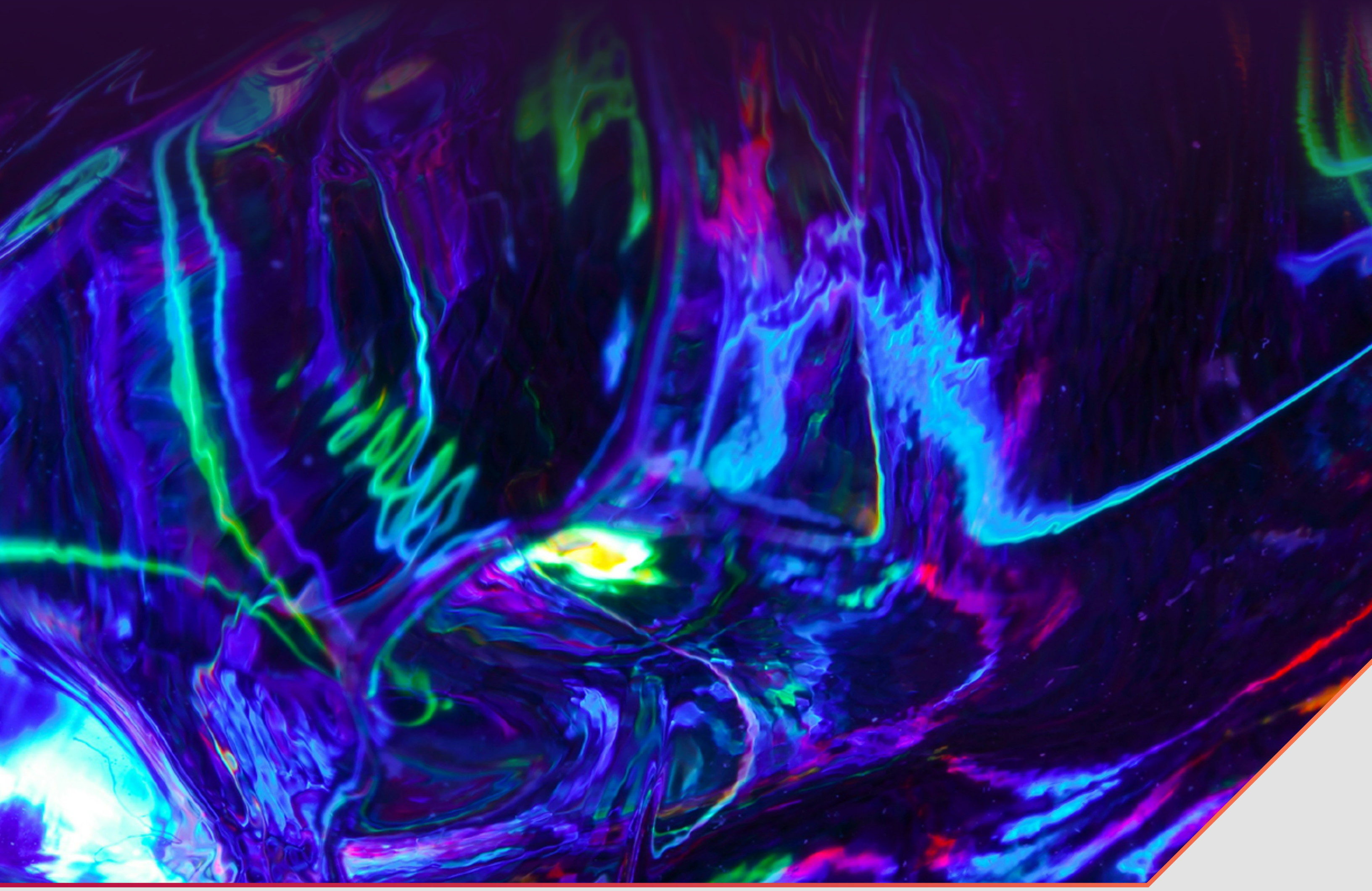
STRIKE
By SecurityScorecard

Massive Botnet Targets M365 with Stealthy Password Spraying Attacks.



SecurityScorecard

Table of Contents

Executive Summary

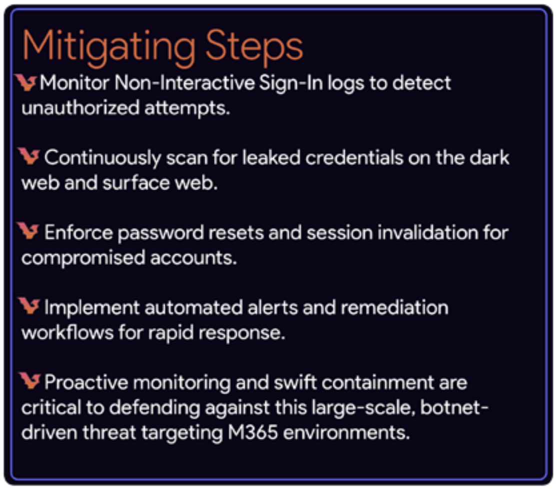
A botnet of over 130,000 compromised devices is conducting large-scale password spraying attacks against Microsoft 365 (M365) accounts, exploiting non-interactive sign-ins with Basic Authentication. This technique bypasses modern login protections and evades MFA enforcement, creating a critical blind spot for security teams. Attackers leverage stolen credentials from infostealer logs to systematically target accounts at scale.

These attacks are recorded in Non-Interactive Sign-In logs, which are often overlooked by security teams. Attackers exploit this gap to conduct high-volume password spraying attempts undetected. This tactic has been observed across multiple M365 tenants globally, indicating a widespread and ongoing threat. As we have seen direct evidence of this behavior in our Non-Interactive Sign-In logs, we encourage anyone operating a M365 tenant to immediately verify whether they are affected, and if so, to rotate credentials belonging to any organization accounts in the logs.

Key Risks

- **Account Takeovers** – Threat actors gain unauthorized access.
- **Business Disruption** – Account lockouts impact operations.
- **Lateral Movement** – Attackers pivot within the network.

Organizations relying solely on interactive sign-in monitoring are **blind to these attacks. Non-interactive sign-ins**, commonly used for service-to-service authentication, legacy protocols (e.g., POP, IMAP, SMTP), and automated processes, **do not trigger MFA** in many configurations. **Basic Authentication**, still enabled in some environments, allows credentials to be transmitted in plain form, making it a prime target for attackers.

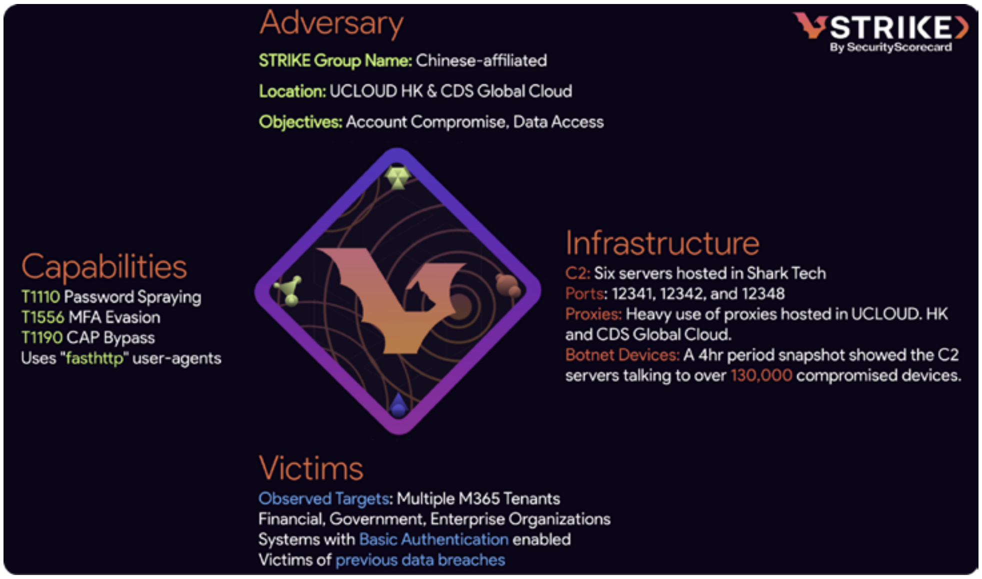


Mitigating Steps

- Monitor Non-Interactive Sign-In logs to detect unauthorized attempts.
- Continuously scan for leaked credentials on the dark web and surface web.
- Enforce password resets and session invalidation for compromised accounts.
- Implement automated alerts and remediation workflows for rapid response.
- Proactive monitoring and swift containment are critical to defending against this large-scale, botnet-driven threat targeting M365 environments.

Microsoft has been progressively deprecating Basic Authentication, with **full retirement of SMTP AUTH planned for September 2025. Despite the ongoing deprecation, the behavior described in this report presents an immediate threat.**

Proactive monitoring and swift containment are **critical to defending against this large-scale, botnet-driven threat** targeting M365 environments.



Adversary

STRIKE Group Name: Chinese-affiliated

Location: UCLOUD HK & CDS Global Cloud

Objectives: Account Compromise, Data Access

Capabilities

T1110 Password Spraying
T1556 MFA Evasion
T1190 CAP Bypass
Uses "fasthttp" user-agents

Infrastructure

C2: Six servers hosted in Shark Tech
Ports: 12341, 12342, and 12348
Proxies: Heavy use of proxies hosted in UCLOUD. HK and CDS Global Cloud.
Botnet Devices: A 4hr period snapshot showed the C2 servers talking to over 130,000 compromised devices.

Victims

Observed Targets: Multiple M365 Tenants
Financial, Government, Enterprise Organizations
Systems with Basic Authentication enabled
Victims of previous data breaches

Disclaimer

Analysis, including ratings and statements, in the content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position, or views of SecurityScorecard or any other entity.

Threat Overview

Threat Actor: Likely a Chinese-affiliated Group (attribution is ongoing).

TTPs: Password spraying, Non-interactive sign-ins, Basic authentication abuse, Use of stolen credentials, Proxy-based evasion.

Target: M365 accounts across multiple organizations.

Infrastructure:

- **Command and Control:** Six servers hosted in Servers Hosting in US
- **Proxies:** Heavy use of proxies hosted in UCLOUD. HK and CDS Global Cloud.
- **Botnet Devices:** A 4hr period snapshot showed the C2 servers talking to over 130,000 compromised devices.

The botnet systematically attempts stolen credentials from infostealer logs across a wide range of M365 accounts, minimizing account lockouts while maximizing the probability of compromise. Non-interactive sign-ins via basic authentication allow the attackers to evade MFA enforcement and potentially bypass Conditional Access Policies (CAP). The attackers have identified a method that causes login events to be logged in the **Non-Interactive Sign-In logs**, which may result in reduced security visibility and response.

Impact

- Account Compromise: Potential unauthorized access to sensitive data, emails, and collaboration tools.
- Business Disruption: Possible account lockouts or service slowdowns due to repeated login attempts.
- Lateral Movement: Use of compromised accounts for internal phishing or further exploitation.
- MFA Evasion: Non-interactive logins bypass MFA enforcement.
- CAP Bypass Potential: Conditional Access Policies may be bypassed depending on implementation.

Indicators of Compromise (IoCs)

Password Spraying:

- Unusual non-interactive login attempts recorded in Non-Interactive Sign-In logs.
- Multiple failed login attempts for a single account from multiple IP addresses.
- User-agent strings associated with automated tools (e.g., “fasthttp”).

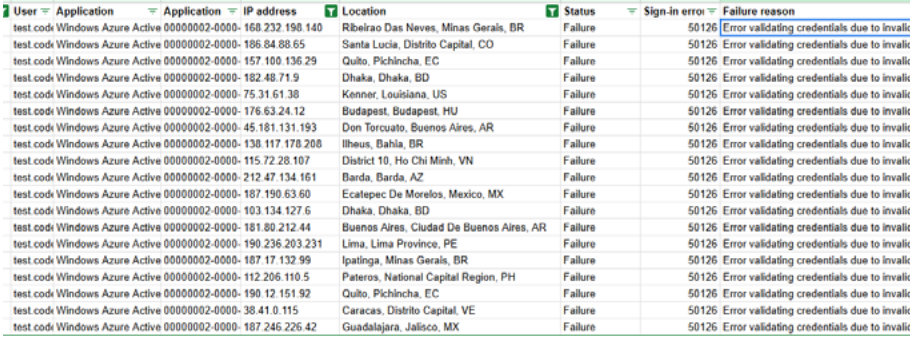
Botnet:

Communications to any of the IPs identified as C2:

70.39.115.74
70.39.120.10
204.188.218.178
204.188.218.179
204.188.210.226
204.188.210.227

Initial Investigation Analysis

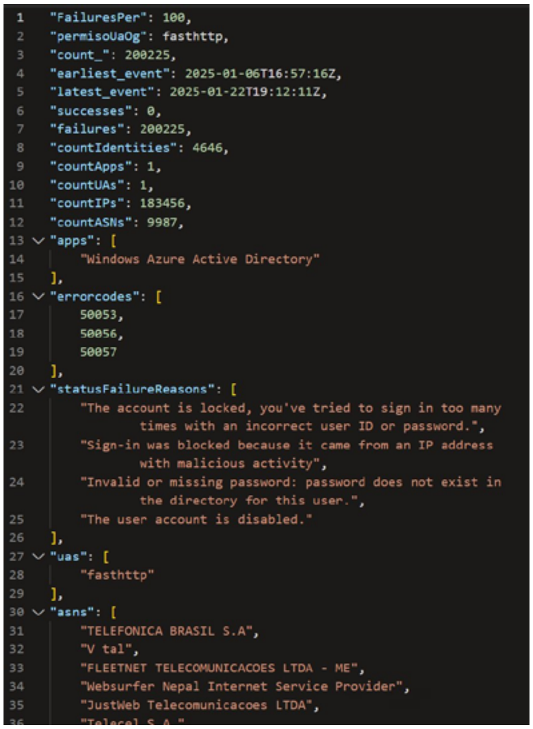
Initial investigation was conducted when a number of failed sign-in attempts were noted in the non-interactive sign-in logs on a Microsoft 365 tenant which the STRIKE team was given access to.



User	Application	Application	IP address	Location	Status	Sign-in erroı	Failure reason
test.cod	Windows Azure Active	00000002-0000-	168.232.198.140	Ribeirao Das Neves, Minas Gerais, BR	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	186.84.88.65	Santa Lucia, Distrito Capital, CO	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	157.100.136.29	Quito, Pichincha, EC	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	182.48.71.9	Dhaka, Dhaka, BD	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	75.31.61.38	Kenner, Louisiana, US	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	176.63.24.12	Budapest, Budapest, HU	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	45.181.131.193	Don Torcuato, Buenos Aires, AR	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	138.117.178.208	Ilheus, Bahia, BR	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	115.72.28.107	District 10, Ho Chi Minh, VN	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	212.47.134.161	Barda, Barda, AZ	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	187.190.63.60	Ecatepec De Morelos, Mexico, MX	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	103.134.127.6	Dhaka, Dhaka, BD	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	181.80.212.44	Buenos Aires, Ciudad De Buenos Aires, AR	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	190.236.203.231	Lima, Lima Province, PE	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	187.17.132.99	Ipatinga, Minas Gerais, BR	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	112.206.110.5	Pateros, National Capital Region, PH	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	190.12.151.92	Quito, Pichincha, EC	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	38.41.0.115	Caracas, Distrito Capital, VE	Failure	50126	Error validating credentials due to invalic
test.cod	Windows Azure Active	00000002-0000-	187.246.226.42	Guadalajara, Jalisco, MX	Failure	50126	Error validating credentials due to invalic

Figure 1. EntraID Non Interactive Sign-in Logs.

Interestingly, the attackers are using basic authentication methods. Events associated with the spraying all use “fasthttp” as the user agent. Searching online highlighted a number of posts talking about the same type of attack we were seeing.



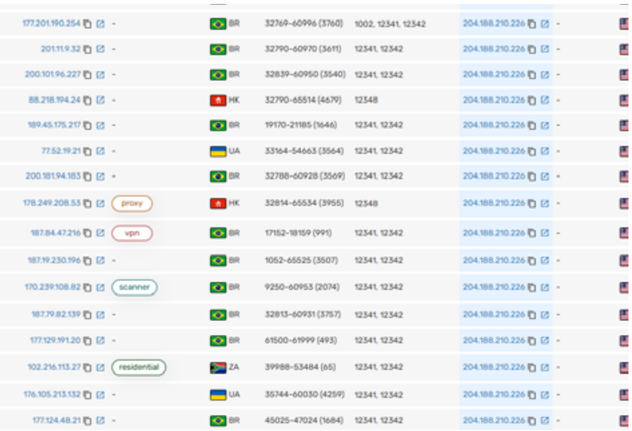
```
"FailuresPer": 100,
"permisoUaOg": fasthttp,
"count_": 200225,
"earliest_event": 2025-01-06T16:57:16Z,
"latest_event": 2025-01-22T19:12:11Z,
"successes": 0,
"failures": 200225,
"countIdentities": 4646,
"countApps": 1,
"countUAs": 1,
"countIPs": 183456,
"countASNs": 9987,
"apps": [
    "Windows Azure Active Directory"
],
"errorcodes": [
    50053,
    50056,
    50057
],
"statusFailureReasons": [
    "The account is locked, you've tried to sign in too many
            times with an incorrect user ID or password.",
    "Sign-in was blocked because it came from an IP address
            with malicious activity",
    "Invalid or missing password: password does not exist in
            the directory for this user.",
    "The user account is disabled."
],
"uas": [
    "fasthttp"
],
"asns": [
    "TELEFONICA BRASIL S.A",
    "V tal",
    "FLEETNET TELECOMUNICACOES LTDA - ME",
    "Websurfer Nepal Internet Service Provider",
    "JustWeb Telecomunicacoes LTDA",
    "Telecel S.A."
```

Figure 2. Twitter post from https://x.com/TekDefense/status/1882151885328810034

A blog post from SpearTip also shows a similar type of attack but no mention of the non-interactive logs.

Netflow Analysis

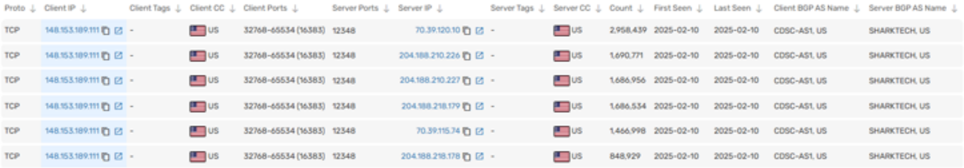
Assessing the netflow data, STRIKE identified recurring IP addresses involved in communication to all attackers' IP addresses.



177.201.190.254	-	BR	32769-60996 (3760)	1002, 12341, 12342	204.188.210.226	-
201.11.9.32	-	BR	32790-60970 (3611)	12341, 12342	204.188.210.226	-
200.101.96.227	-	BR	32839-60950 (3540)	12341, 12342	204.188.210.226	-
88.218.194.24	-	HK	32790-65514 (4679)	12348	204.188.210.226	-
189.45.175.217	-	BR	19170-21185 (1646)	12341, 12342	204.188.210.226	-
77.52.19.21	-	UA	33164-54663 (3564)	12341, 12342	204.188.210.226	-
200.181.94.183	-	BR	32788-60928 (3569)	12341, 12342	204.188.210.226	-
178.249.208.53	proxy	HK	32814-65534 (3955)	12348	204.188.210.226	-
187.84.47.216	vpn	BR	17152-18159 (991)	12341, 12342	204.188.210.226	-
187.19.230.196	-	BR	1052-65525 (3507)	12341, 12342	204.188.210.226	-
170.239.108.82	scanner	BR	9250-60953 (2074)	12341, 12342	204.188.210.226	-
187.79.82.139	-	BR	32813-60931 (3757)	12341, 12342	204.188.210.226	-
177.129.191.20	-	BR	61500-61999 (493)	12341, 12342	204.188.210.226	-
102.216.113.27	residential	ZA	39988-53484 (65)	12341, 12342	204.188.210.226	-
176.105.213.132	-	UA	35744-60030 (4259)	12341, 12342	204.188.210.226	-
177.124.48.21	-	BR	45025-47024 (1684)	12341, 12342	204.188.210.226	-

Figure 3. Common communication with compromised hosts.

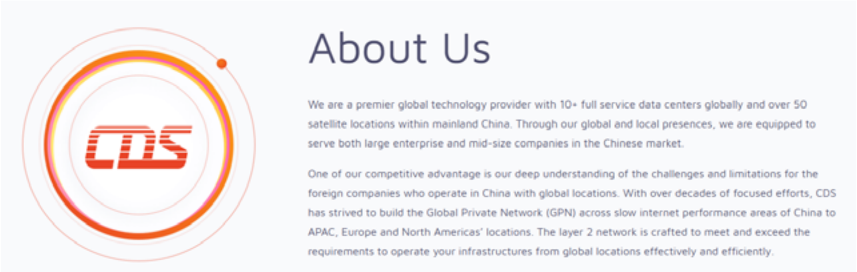
This IP address (204.188.210.226) is hosted at Servers Hosting in US. The majority of traffic associated with this netflow was occurring over ports 12341 and 12342, there was also another port being used less frequently (12348). Further investigation revealed that this other port is seen being used by 6 different servers. Assessment of IPs talking to the same 6 IP addresses over the same port highlighted two primary hosting providers being used. Both have affiliation with China. CDSC-AS1 and UCLOUD HK.



Proto	Client IP	Client Tags	Client CC	Client Ports	Server Ports	Server IP	Server Tags	Server CC	Count	First Seen	Last Seen	Client BGP AS Name	Server BGP AS Name
TCP	148.153.189.111	-	US	32768-65534 (16383)	12348	70.39.120.10	-	US	2,958,439	2025-02-10	2025-02-10	CDSC-AS1, US	SHARKTECH, US
TCP	148.153.189.111	-	US	32768-65534 (16383)	12348	204.188.210.226	-	US	1,690,771	2025-02-10	2025-02-10	CDSC-AS1, US	SHARKTECH, US
TCP	148.153.189.111	-	US	32768-65534 (16383)	12348	204.188.210.227	-	US	1,686,956	2025-02-10	2025-02-10	CDSC-AS1, US	SHARKTECH, US
TCP	148.153.189.111	-	US	32768-65534 (16383)	12348	204.188.218.179	-	US	1,686,534	2025-02-10	2025-02-10	CDSC-AS1, US	SHARKTECH, US
TCP	148.153.189.111	-	US	32768-65534 (16383)	12348	70.39.115.74	-	US	1,466,998	2025-02-10	2025-02-10	CDSC-AS1, US	SHARKTECH, US
TCP	148.153.189.111	-	US	32768-65534 (16383)	12348	204.188.218.178	-	US	848,929	2025-02-10	2025-02-10	CDSC-AS1, US	SHARKTECH, US

Figure 4. CDSC-AS1 Hosted server communicating with C2 servers.

CDS Cloud is a cloud provider with links to China.

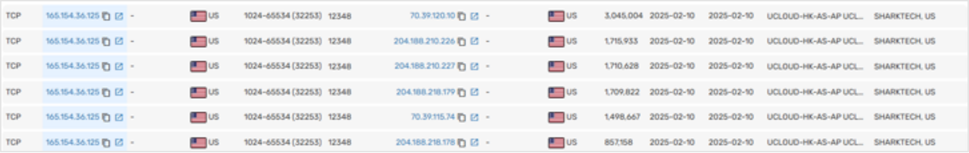


About Us

We are a premier global technology provider with 10+ full service data centers globally and over 50 satellite locations within mainland China. Through our global and local presences, we are equipped to serve both large enterprise and mid-size companies in the Chinese market.

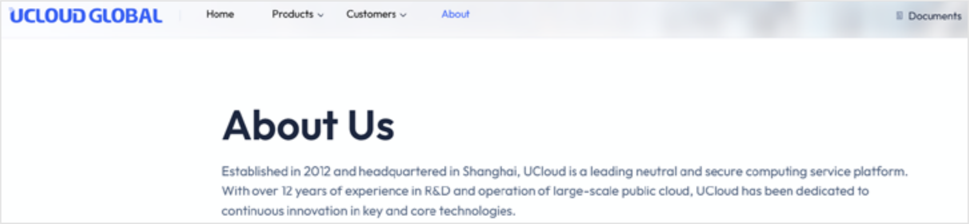
One of our competitive advantage is our deep understanding of the challenges and limitations for the foreign companies who operate in China with global locations. With over decades of focused efforts, CDS has strived to build the Global Private Network (GPN) across slow internet performance areas of China to APAC, Europe and North Americas' locations. The layer 2 network is crafted to meet and exceed the requirements to operate your infrastructures from global locations effectively and efficiently.

Figure 5. CDS Cloud Company Information



TCP	165.154.36.125	-	US	1024-65534 (32253)	12348	70.39.120.10	-	US	3,045,004	2025-02-10	2025-02-10	UCLOUD-HK-AS-AP UCL...	SHARKTECH, US
TCP	165.154.36.125	-	US	1024-65534 (32253)	12348	204.188.210.226	-	US	1,715,933	2025-02-10	2025-02-10	UCLOUD-HK-AS-AP UCL...	SHARKTECH, US
TCP	165.154.36.125	-	US	1024-65534 (32253)	12348	204.188.210.227	-	US	1,710,628	2025-02-10	2025-02-10	UCLOUD-HK-AS-AP UCL...	SHARKTECH, US
TCP	165.154.36.125	-	US	1024-65534 (32253)	12348	204.188.218.179	-	US	1,709,822	2025-02-10	2025-02-10	UCLOUD-HK-AS-AP UCL...	SHARKTECH, US
TCP	165.154.36.125	-	US	1024-65534 (32253)	12348	70.39.115.74	-	US	1,498,667	2025-02-10	2025-02-10	UCLOUD-HK-AS-AP UCL...	SHARKTECH, US
TCP	165.154.36.125	-	US	1024-65534 (32253)	12348	204.188.218.178	-	US	857,158	2025-02-10	2025-02-10	UCLOUD-HK-AS-AP UCL...	SHARKTECH, US

Figure 6. UCLOUD HK Hosted server communicating with C2 servers.



About Us

Established in 2012 and headquartered in Shanghai, UCloud is a leading neutral and secure computing service platform. With over 12 years of experience in R&D and operation of large-scale public cloud, UCloud has been dedicated to continuous innovation in key and core technologies.

Figure 6. UCLOUD HK Hosted server communicating with C2 servers.

Context on the Servers Hosting in US Server

Servers Hosting in US had an “F” rating in the SecurityScorecard TPRM platform. An “F” rating correlates over 14 times higher to a risk of breach than an “A” rating. However, in this case, it is clear the rating is a better indication of the rampant malicious activity being carried out by customers of the platform. In particular, there are at least 11 IP addresses on a majority of openly available IP blocklists, 246 IPs running SMTP on non-standard ports, and 274 potentially unwanted applications/trackers being hosted. The trackers in particular we also observed on the netflow logs between the aforementioned servers.

C2 Server Investigation

The 6 identified C2 servers have similar ports open:

Port	Service	Possible Use
1002	Unassigned (Often RPC related)	Unknown
2181	Zookeeper	Likely managing a Kafka distributed botnet setup
3306	MySQL	Could store stolen data or botnet configuration
6379	Redis	Potential key-value store for botnet related tasking
7779	Unknown	Unknown
8081	Jetty web service	Zookeeper query service
10050	Zabbix Agent	Potential botnet monitoring
33060	MySQL X Protocol	Likely used with MySQL service

In addition to the services above, the following table of ports is common across all identified C2 servers:

Port	Possible Use
12341	Likely Botnet C2 channel (Client Registration)
12342	Possibly used for tasking infected hosts
12347	Possible data exfil or backup C2
12348	High probability of main C2 command execution

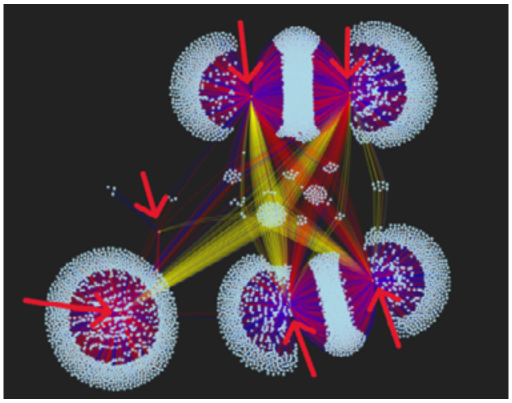
The following image shows a subset of netflow data (taken from the top 5000 active IPs), the color of connecting lines denoting the port used Red:12341, Blue:12342, Yellow:12348. The yellow nodes (red arrows) are the suspected C2 servers, while the light blue nodes are compromised devices.

These servers are running Apache Zookeeper, a distributed system coordination framework, which would indicates a likely technology choice to run a distributed campaign. It is worth noting that the use of Zookeeper, an industry-standard for distributed systems development, could indicate a sophisticated threat actor with strong software engineering knowledge, given the complexity of running a Zookeeper cluster at scale. Access to port 8081 is not restricted and it was possible to query the servers to establish further details including uptime. Analysis of the nodes available from zookeeper suggests that these are also running Apache Kafka.

While the Servers Hosting in US servers are hosted in the US, the timezone for the servers has been configured as “Asia/Shanghai.”

Traffic Frequency Analysis (C2 Servers)

Traffic patterns to the C2 ports show high correlation to the CDS Global Cloud and UCLOUD IPs.

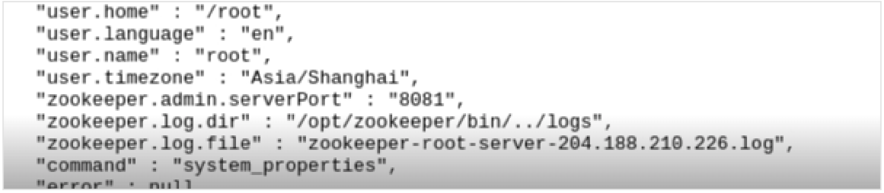


Traffic Timeline Analysis (C2 Traffic)

Botnet traffic to the suspected C2 ports was plotted against a timeline. The results show a clear indication of beaconing between C2 servers and other devices.

Server Uptimes

Based on server uptime it appears that the botnet has been up and running since Dec 2024.



```
  "user.home" : "/root",
  "user.language" : "en",
  "user.name" : "root",
  "user.timezone" : "Asia/Shanghai",
  "zookeeper.admin.serverPort" : "8081",
  "zookeeper.log.dir" : "/opt/zookeeper/bin/../logs",
  "zookeeper.log.file" : "zookeeper-root-server-204.188.210.226.log",
  "command" : "system_properties",
  "error" : null
```

Figure 9. Server timezone set to “Asia/Shanghai”

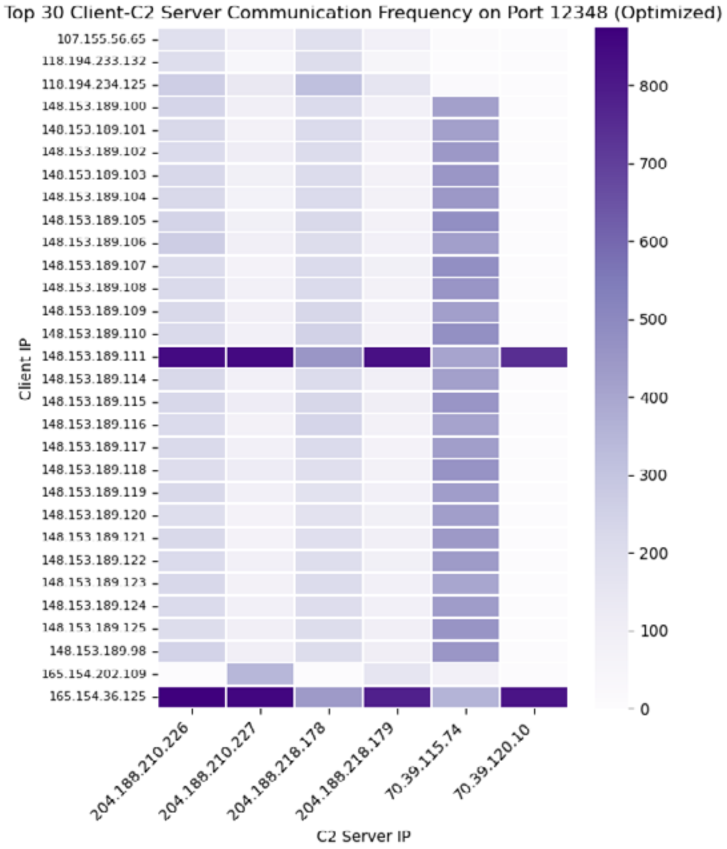


Figure 10. Conversation frequency between IPs and C2 servers on port 12348

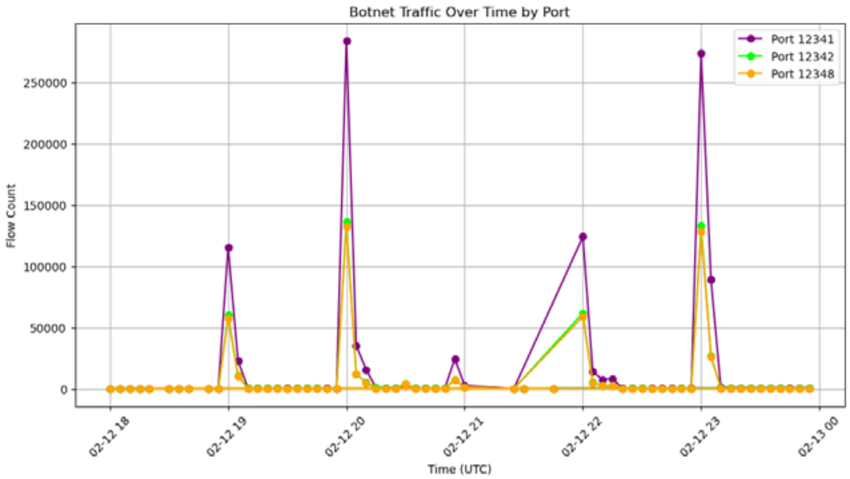
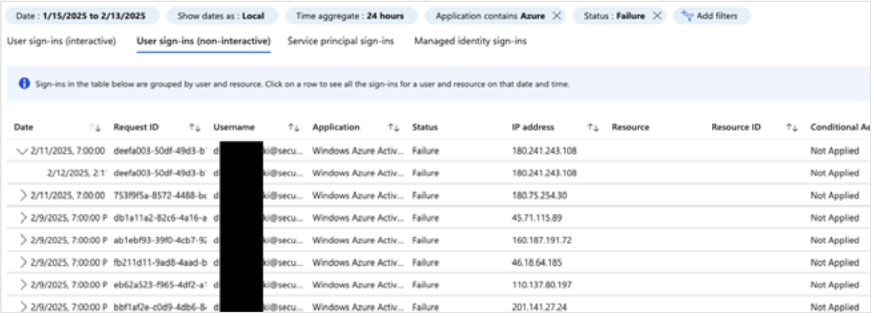


Figure 11. Timeline of traffic for all suspected C2 ports

Linkage of Users to Infostealer Logs

A correlation of the identified users STRIKE have seen in the non-interactive logs to breached credentials has shown hits for affected users.

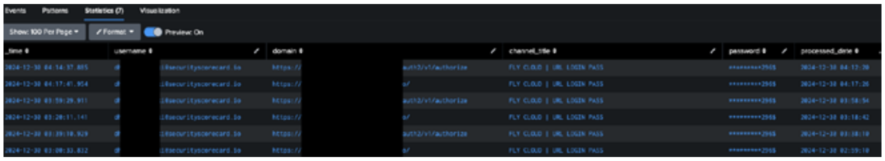
IP	Est. Powered On Date
70.39.115.74	2024-12-04
70.39.120.10	2024-12-04
204.188.218.178	2024-12-01
204.188.218.179	2024-12-01
204.188.210.226	2024-12-30
204.188.210.227	2024-12-30



Date : 1/15/2025 to 2/13/2025
Show dates as : Local
Time aggregate : 24 hours
Application contains Azure
Status : Failure
Add filters
User sign-ins (interactive)
User sign-ins (non-interactive)
Service principal sign-ins
Managed identity sign-ins

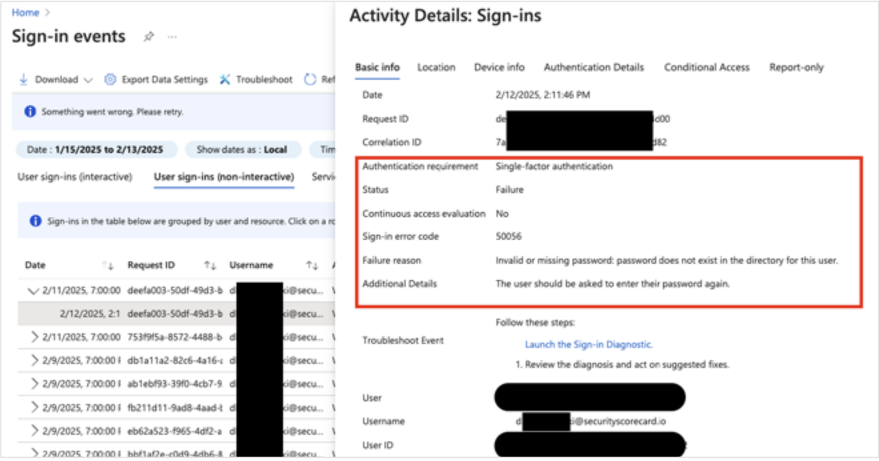
Sign-ins in the table below are grouped by user and resource. Click on a row to see all the sign-ins for a user and resource on that date and time.

Date	Request ID	Username	Application	Status	IP address	Resource	Resource ID	Conditional Ac
2/11/2025, 7:00:00	deefa003-50df-49d3-b	d[redacted]ki@secu...	Windows Azure Activ...	Failure	180.241.243.108			Not Applied
2/12/2025, 2:1	deefa003-50df-49d3-b	d[redacted]ki@secu...	Windows Azure Activ...	Failure	180.241.243.108			Not Applied
2/11/2025, 7:00:00	753f9f5a-8572-4488-bc	d[redacted]ki@secu...	Windows Azure Activ...	Failure	180.75.254.30			Not Applied
2/9/2025, 7:00:00 P	db1a11a2-82c6-4a16-a	d[redacted]ki@secu...	Windows Azure Activ...	Failure	45.71.115.89			Not Applied
2/9/2025, 7:00:00 P	ab1ebf93-39f0-4cb7-9	d[redacted]ki@secu...	Windows Azure Activ...	Failure	160.187.191.72			Not Applied
2/9/2025, 7:00:00 P	fb211d11-9ad8-4aad-b	d[redacted]ki@secu...	Windows Azure Activ...	Failure	46.18.64.185			Not Applied
2/9/2025, 7:00:00 P	eb62a523-f965-4df2-a	d[redacted]ki@secu...	Windows Azure Activ...	Failure	110.137.80.197			Not Applied
2/9/2025, 7:00:00 P	bbf1af2e-c0d9-4db6-8	d[redacted]ki@secu...	Windows Azure Activ...	Failure	201.141.27.24			Not Applied



```
_time                     username                              domain                                   channel_title                 password        processed_date
2024-12-30 04:14:37.885   d[redacted]i@securityscorecard.io     https://[redacted]auth2/v1/authorize     FLY CLOUD | URL LOGIN PASS    *********2965   2024-12-30 04:12:20
2024-12-30 04:17:41.954   d[redacted]i@securityscorecard.io     https://[redacted]o/                     FLY CLOUD | URL LOGIN PASS    *********2965   2024-12-30 04:17:26
2024-12-30 03:59:29.911   d[redacted]i@securityscorecard.io     https://[redacted]auth2/v1/authorize     FLY CLOUD | URL LOGIN PASS    *********2965   2024-12-30 03:58:54
2024-12-30 03:20:11.141   d[redacted]i@securityscorecard.io     https://[redacted]o/                     FLY CLOUD | URL LOGIN PASS    *********2965   2024-12-30 03:18:42
2024-12-30 03:39:10.929   d[redacted]i@securityscorecard.io     https://[redacted]auth2/v1/authorize     FLY CLOUD | URL LOGIN PASS    *********2965   2024-12-30 03:38:10
2024-12-30 03:00:33.832   d[redacted]i@securityscorecard.io     https://[redacted]o/                     FLY CLOUD | URL LOGIN PASS    *********2965   2024-12-30 02:59:10
```

Figure 12. Matching EntraID logs to Infostealer logs from SecurityScorecard's Threat Intelligence sources



Something went wrong. Please retry.

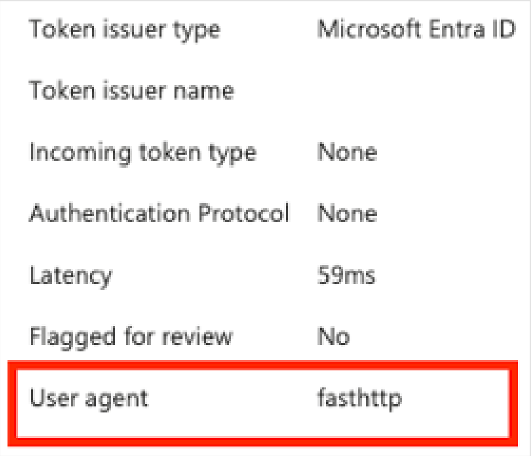
Sign-ins in the table below are grouped by user and resource. Click on a r

Date	Request ID	Username
2/11/2025, 7:00:00	deefa003-50df-49d3-b	d[redacted]i@secu...
2/12/2025, 2:1	deefa003-50df-49d3-b	d[redacted]i@secu...
2/11/2025, 7:00:00	753f9f5a-8572-4488-b	d[redacted]i@secu...
2/9/2025, 7:00:00 I	db1a11a2-82c6-4a16-a	d[redacted]i@secu...
2/9/2025, 7:00:00 I	ab1ebf93-39f0-4cb7-9	d[redacted]i@secu...
2/9/2025, 7:00:00 I	fb211d11-9ad8-4aad-b	d[redacted]i@secu...
2/9/2025, 7:00:00 I	eb62a523-f965-4df2-a	d[redacted]i@secu...
2/9/2025, 7:00:00 I	bbf1af2e-c0d9-4db6-8	d[redacted]i@secu...

Activity Details: Sign-ins

Date	2/12/2025, 2:11:46 PM
Request ID	de[redacted]c00
Correlation ID	7a[redacted]d82
Authentication requirement	Single-factor authentication
Status	Failure
Continuous access evaluation	No
Sign-in error code	50056
Failure reason	Invalid or missing password: password does not exist in the directory for this user.
Additional Details	The user should be asked to enter their password again.
Troubleshoot Event	Follow these steps: Launch the Sign-in Diagnostic. 1. Review the diagnosis and act on suggested fixes.
User	[redacted]
Username	d[redacted]i@securityscorecard.io
User ID	[redacted]

Figure 13. Basic Authentication in Non-Interactive logs



Token issuer type	Microsoft Entra ID
Token issuer name	
Incoming token type	None
Authentication Protocol	None
Latency	59ms
Flagged for review	No
User agent	fasthttp

Figure 14. User Agent string of "fasthttp"

Conclusion

OThis botnet activity highlights the importance of deprecating basic authentication, proactively monitoring login patterns, and implementing strong detection mechanisms for password spraying attempts. The attackers' use of **Non-Interactive Sign-In** logs to evade MFA and possibly Conditional Access Policies underscores the need for organizations to reassess their authentication strategies. Additionally, organizations should monitor for leaked credentials on underground forums and swiftly act to reset compromised accounts.

Contact STRIKE for Incident Response

If you suspect your organization has been impacted by this activity, contact the STRIKE Incident Response team immediately. Our experts provide:

- Rapid Containment: Minimize damage and halt ongoing breaches.
- Forensic Analysis: Understand how attackers gained access and what data was affected.
- Strategic Guidance: Strengthen your security posture against evolving threats.

Proactively Mitigate Supply Chain Risks

To protect your organization from future supply chain attacks, SecurityScorecard's Supply Chain Detection and Response (SCDR) solution offers the tools to:

- Monitor and assess your software supply chain for vulnerabilities.
- Detect suspicious activity across your development pipelines.
- Receive actionable insights to prevent advanced threats like "Phantom Circuit."

Take control of your supply chain security today. Contact us for assistance or to learn more about SCDR and incident response services.

For STRIKE media inquiries, contact us here.