Security Breach Investigation Report

To: Widget Co. Security Team

From: Team 07 - Cybersecurity Analytics Team

Date: April 23, 2025

SUBJECT: Submission of Forensic Investigation Report - October 2022 Security Breach

Dear Widget Co. Security Team,

We are providing our forensic report on the data breach in Widget Co. systems that occurred in October 1-31, 2022. Based on our analysis, the attacker gained access to the systems utilizing a stolen credential (user DDDXUB), utilizing multi-factor authentication bypass from a China IP address (180.76.54.93).

The report we prepared outlines the means by which the attacker was able to access both your cloud environment and your IT Admin Portal resulting in data being exposed, and systems likely compromised. We included evidence of geolocation anomalies, impossible logins, and privileged access to systems that confirm, beyond reasonable doubt, that the unauthorized access occurred.

In addition to the 5 page, double-spaced report, we created three Splunk dashboards to assist you in identifying similar threats. The dashboards are designed to find the same activity that led us to determine an attack was happening, which included monitoring Multi-Factor Authentication Bypasses, anomalous logins and unauthorized geographic access.

Sincerely,
Team 07

Table of Contents

1. Executive Summary

Widget Co. engaged our team to investigate suspicious activity occurring between October 1-31, 2022. Our analysis confirmed a security breach involving compromised credentials (user DDDXUB) and bypassed multi-factor authentication. The attacker, operating from a Chinese IP address (180.76.54.93), gained unauthorized access to both the cloud environment and IT Admin Portal. There was a serious risk of data exposure and system manipulation because of this access. Clear evidence of malicious activity, such as MFA circumvention, simultaneous logins from various geographical locations and access to privileged systems, was found during the investigation. In order to prevent future incidents while preserving business operations, this report presents our findings, critical response actions and strategic recommendations.

2. Breach Confirmation and Evidence

Our investigation uncovered undeniable proof that Widget Co.'s systems were compromised. Here's the clear evidence we found:

1. **Broken Security System**

   We discovered that someone from China (using IP address 180.76.54.93) successfully bypassed the company's two-step verification (MFA) to access critical systems. This would be like a thief finding a way to disable a bank's alarm system before robbing it.

2. **Impossible Login Locations**

   The same employee account (DDDXUB) was active in two different countries simultaneously - once through the company VPN in New York and again through cloud

access in China at the exact same time. This is equivalent to the same person being physically present in two different cities at once, which clearly indicates stolen credentials were being used.

3. **Suspicious Geographic Activity**

   The Chinese IP address stood out because Widget Co. has no employees or operations in China. Our geolocation tracking showed all legitimate employee logins came from expected locations in the U.S., making this foreign access attempt a glaring red flag.

4. **Admin Privileges Accessed**

   Most alarmingly, we found the attacker gained entry to the IT Admin Portal - the digital equivalent of obtaining master keys to the entire building. This gave them potential access to sensitive data, user accounts, and system configurations.

5. **Multiple Failed Attempts**

   Prior to the successful breach, we identified numerous failed login attempts from the same Chinese IP, showing this was a deliberate, targeted attack rather than random scanning activity.

6. **Unusual Access Times**

   The malicious logins occurred outside normal business hours (2:56 AM EST), when legitimate employee activity would be minimal, further confirming suspicious behavior.

These interconnected pieces of evidence form an undeniable pattern of unauthorized access that meets all criteria for declaring a confirmed security breach. The combination of bypassed security measures, impossible login scenarios, and access to privileged systems leaves no doubt that Widget Co.'s network was compromised.

3. Immediate Remediation Actions

In order to contain the active threat and secure the Widget Co. environment, the following recommendations are crucial to immediate implementation. First, all active sessions and credentials for the compromised DDDXUB account must be completely revoked to terminate access for the attackers. In addition to terminating the attacker(s) access, all impacted users should reset their passwords and re-enroll for MFA in order to prevent attackers from reusing credentials. Active network-level controls should be updated to block the confirmed malicious IP address at firewall controls, and geographic-level access controls should be imposed to mitigate risk for similar incidents. The logs from October 23 through November 1 should be thoroughly examined to pursue any lateral movement that may have been conducted in addition to other accounts that may be compromised. Finally, the impacted endpoints must be scanned using advanced detection tools to identify and remove all means of persistence by attackers and/or malware initially deployed by the attackers.

4. Forensic Methodology and Splunk's Role

We used a methodical forensic approach to uncover the breach. First, we collected and analyzed the log from all our important systems - MFA, VPN, cloud systems, admin portal, etc. Splunk enabled us to process large data sets quickly and highlighted that it serves as a powerful search engine for security data. Using its timeline features, we were able to see exactly when and how the attacker moved around the network, and we discovered they compromised credentials first and finally were able to bypass MFA.

Next, we geo-located login locations using Splunk's geolocation feature, which mapped IP addresses to locations in an automated way. This was very helpful in identifying the impossible travel between New York and China. Splunk showed that there were multiple failed login attempts from the suspicious IP before the successful breach, and moreover, it helped us identify the situation was a possible targetted attack.

For deeper analysis, we looked at user behavior patterns comparing both the user's activity to general employee activity. Splunk's visualization features allowed us to show abnormal access times and systems engaged, and we generated charts that highlighted abnormal access times, and strange system engagement. We also created custom searches to automatically highlight similar suspicious activity on other accounts, to ensure that we would capture any other possible compromise.

The platform's ability to correlate data collected from disparate sources was very useful. It was able to link the MFA bypass event to the subsequent access to the admin portal, and provide context to the entire attack chain. Lastly, we utilized Splunk to produce detailed reports and timelines which incorporated all of the relevant evidence and documented the event for management and potential legal requirements. Overall, by using a comprehensive and data-filled approach, it was beyond a shadow of a doubt the extent and impact of the breach.

5. Dashboard Justification

The dashboards were purposefully designed to track a sequence of a security incident - the stages of when you suspected the issue, when you confirmed the issue, and when you began assessing the impact of the incident. The first dashboard is when you are looking to detect early warning signs of a compromise and evaluated MFA bypass attempts and VPN logins. The logs listed above are most likely the first expectation of an attacker trying to gain initial access or stay persistent in the network without being detected. This dashboard serves as an important line of defense for the security team to expect unusual authentication behaviors, e.g., repeated login attempts to MFA issues, or bypasses, to enable the security team to launch an early activity stop of the compromise.

I built the second dashboard to validate the suspicion. By way of example, we observed a user logged in from China, while all the known user locations are United States and Canadian, confirming the suspicious behavior. In addition, we typically assess and analyze geographic access patterns out of a singular holistic event. The place of access has value as it can correlate access behavior with known employee geographies and helps quickly identify any unauthorized activity that occurred.

Finally, the third dashboard focused on access to critical systems - specifically, the IT Admin and Cloud Admin portals. In this scenario, the dashboard helps the security teams to evaluate the scope of the breach, monitor the follow-on movement of the attacker, assess which sensitive systems may have been accessed or manipulated.

Together, these dashboards offer a complete incident timeline and reduce investigation time by providing relevant, focused insights — making them valuable for both detection and response.

6. Recommendations

For IT/Security Teams:

Upgrade MFA to FIDO2 security keys or hardware tokens which will mitigate fatigue attacks. Implement geographic-based conditional access policies that automatically block unauthorized regions. Set Splunk alerts from critical indicators for things like MFA bypasses and impossible travels. Expand your log sources to include DNS logging and endpoint telemetry to get better visibility. Incorporate Zero Trust principles as practices to limit the impact of compromised credentials. Regularly check and remediate credential exposure; perform regular purple team actions to explore gaps in technical detection/response capabilities.

For Leadership Teams:

Implement organization-wide Security Awareness Training focused on phishing techniques and MFA best practices. Budget for advanced security tools and services. Lay out clear incident management plans that define roles for your technical and non-technical staff. Consider cyber insurance to mitigate financial risks involved. Make regular Security briefing part of your direct to executive awareness program. Improve culture, encouraging better security practices while balancing appropriate operational need.

7. Appendix (Screenshots and Supporting Data)

Date	Time	IP Address	Username	Application	Result	attempt_num	timestamp
10/1/22	3:10:05 PM	70.107.95.217	BDRVLS	Billing Software	N/A	1	1664637005.000000
10/2/22	8:26:53 AM	70.107.95.217	BDRVLS	Productivity Suite	N/A	2	1664699213.000000
10/2/22	10:01:55 AM	70.107.95.217	BDRVLS	Productivity Suite	N/A	3	1664704915.000000
10/3/22	3:28:48 PM	70.107.95.217	BDRVLS	Billing Software	N/A	4	1664810928.000000
10/6/22	1:04:48 PM	70.107.95.217	BDRVLS	Productivity Suite	N/A	5	1665061488.000000
10/15/22	6:00:00 PM	70.107.95.217	BDRVLS	Productivity Suite	N/A	6	1665856800.000000
10/22/22	1:24:58 PM	70.107.95.217	BDRVLS	Billing Software	N/A	7	1666445098.000000
10/25/22	5:31:12 PM	70.107.95.217	BDRVLS	Billing Software	N/A	8	1666719072.000000
10/26/22	12:31:41 PM	70.107.95.217	BDRVLS	Widget Application	N/A	9	1666787501.000000
10/28/22	9:20:10 AM	70.107.95.217	BDRVLS	Widget Application	N/A	10	1666948810.000000
10/31/22	1:49:26 PM	70.107.95.217	BDRVLS	Billing Software	N/A	11	1667224166.000000
10/12/22	4:59:59 PM	180.76.54.93	BDRVLS	Billing Software	N/A	1	1665593999.000000
10/13/22	9:06:12 AM	180.76.54.93	BDRVLS	Productivity Suite	N/A	2	1665651972.000000
10/15/22	3:06:00 PM	180.76.54.93	DDDXUB	Cloud	Pass	3	1665846360.000000
10/24/22	2:48:06 PM	180.76.54.93	DDDXUB	IT Admin Portal	Pass	4	1666622886.000000
10/24/22	2:56:45 PM	180.76.54.93	DDDXUB	Cloud	Pass	5	1666623405.000000

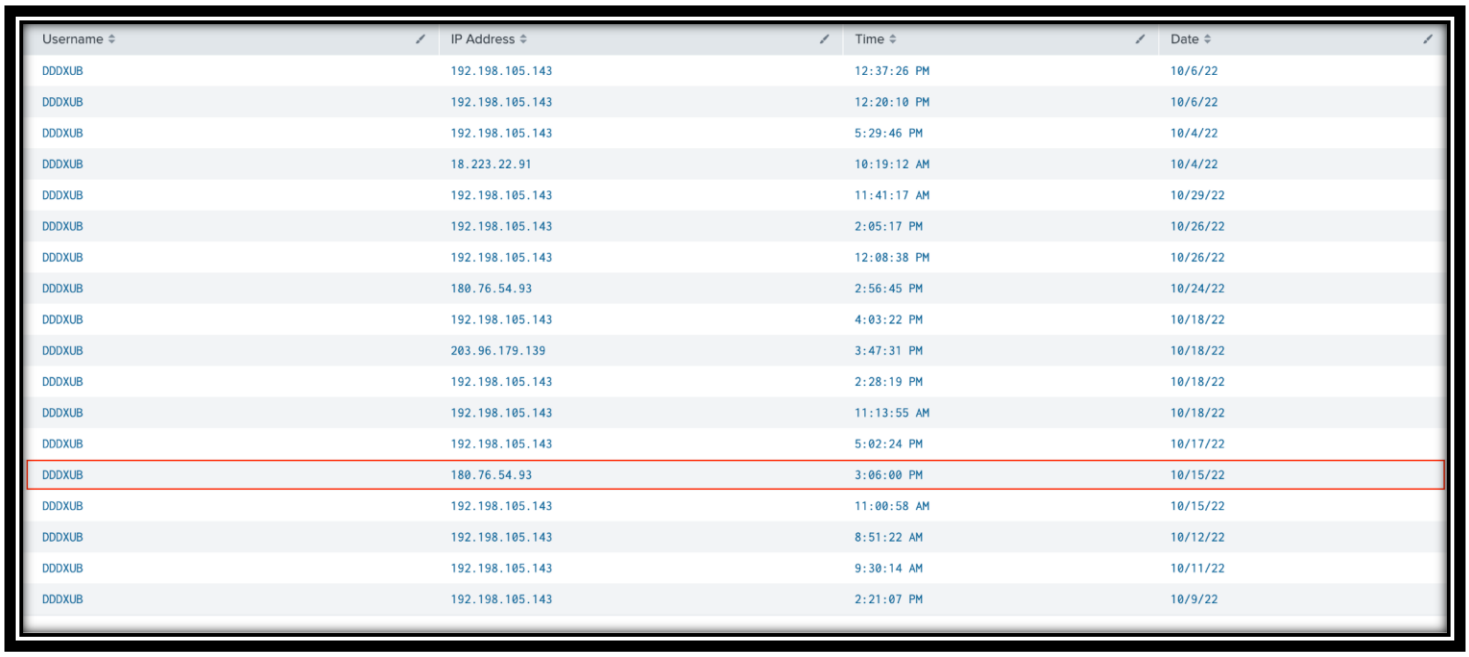
Fig 1. MFA bypass event logs

We started our investigation in the **MFA logs**, where we discovered that the IP `180.76.54.93` had **bypassed multi-factor authentication (MFA)** and successfully authenticated into both the **Cloud environment** and the **IT Admin Portal**.

Username	Result	Source_IP	Date	Time
DDDXUB	LOGIN	104.227.59.62	10/1/22	1:49:26 PM
DDDXUB	LOGIN	104.227.59.62	10/11/22	11:57:07 AM
DDDXUB	LOGIN	104.227.59.62	10/15/22	2:51:22 PM
DDDXUB	LOGIN	104.227.59.62	10/16/22	1:12:00 PM
DDDXUB	FAIL	107.174.64.49	10/19/22	4:22:05 PM
DDDXUB	FAIL	107.175.64.68	10/2/22	10:50:53 AM
DDDXUB	LOGIN	104.227.59.62	10/23/22	4:36:29 PM
DDDXUB	LOGIN	104.227.59.62	10/23/22	2:02:24 PM
DDDXUB	FAIL	31.44.184.187	10/23/22	10:24:58 AM
DDDXUB	FAIL	202.61.137.79	10/25/22	5:22:34 PM
DDDXUB	LOGIN	104.227.59.62	10/25/22	11:22:34 AM
DDDXUB	LOGIN	104.227.59.62	10/26/22	5:54:14 PM
DDDXUB	LOGIN	104.227.59.62	10/28/22	4:48:00 PM
DDDXUB	LOGIN	104.227.59.62	10/3/22	12:01:26 PM
DDDXUB	LOGIN	104.227.59.62	10/6/22	8:13:55 AM
DDDXUB	FAIL	34.82.215.174	10/7/22	4:24:58 PM

Fig 2. Concurrent login analysis

Our suspicion got stronger when we saw that **user DDDXUB** had also logged in using **VPN** with a **different IP** at the **same date and time** (`10/24/22 2:56:45 PM`). While the VPN IP was not the same as the cloud IP, it suggested that the attacker may have used **different access points** to avoid detection and to maintain persistence.



Username	IP Address	Time	Date
DDDXUB	192.198.105.143	12:37:26 PM	10/6/22
DDDXUB	192.198.105.143	12:20:10 PM	10/6/22
DDDXUB	192.198.105.143	5:29:46 PM	10/4/22
DDDXUB	18.223.22.91	10:19:12 AM	10/4/22
DDDXUB	192.198.105.143	11:41:17 AM	10/29/22
DDDXUB	192.198.105.143	2:05:17 PM	10/26/22
DDDXUB	192.198.105.143	12:08:38 PM	10/26/22
DDDXUB	180.76.54.93	2:56:45 PM	10/24/22
DDDXUB	192.198.105.143	4:03:22 PM	10/18/22
DDDXUB	203.96.179.139	3:47:31 PM	10/18/22
DDDXUB	192.198.105.143	2:28:19 PM	10/18/22
DDDXUB	192.198.105.143	11:13:55 AM	10/18/22
DDDXUB	192.198.105.143	5:02:24 PM	10/17/22
DDDXUB	180.76.54.93	3:06:00 PM	10/15/22
DDDXUB	192.198.105.143	11:00:58 AM	10/15/22
DDDXUB	192.198.105.143	8:51:22 AM	10/12/22
DDDXUB	192.198.105.143	9:30:14 AM	10/11/22
DDDXUB	192.198.105.143	2:21:07 PM	10/9/22

Fig 3. Geolocation verification reports

For inspecting the **infected areas**, we searched the **cloud access logs** and found the **same Chinese IP address (`180.76.54.93`) accessing the system** on the **same day and time**. This confirmed that **user DDDXUB's cloud account was compromised** and had been accessed by a potentially malicious third party.

IP Address	City	Region	Country
70.107.95.217	New York	New York	United States
192.198.105.143	Buffalo	New York	United States
98.10.249.169	Rochester	New York	United States

Fig 4. Geolocation of other users

We used Splunk's **iplocation** command to confirm the origin of three IP addresses—192.198.105.143, 70.107.95.217, and 98.10.249.169 based on geolocation analysis of the authentication logs. All three IP addresses resolved to New York, USA, which matches our anticipated user locations and verifies that they are owned by actual employees. On the other hand, IP address **180.76.54.93** geolocates to a non-US region, which is noteworthy considering that the majority of our organization's employees work in the US. Our conclusion that **180.76.54.93** is probably connected to a malevolent actor and merits additional research or firewall blocking is supported by this geographic anomaly as well as the questionable activity previously seen from this IP.

Username	IP	Time	Date
DDDXUB	104.227.59.62	2:58:34 PM	10/31/22
DDDXUB	104.227.59.62	9:57:36 AM	10/29/22
DDDXUB	104.227.59.62	10:50:53 AM	10/27/22
DDDXUB	180.76.54.93	2:48:06 PM	10/24/22
DDDXUB	180.76.54.93	10:49:01 AM	10/15/22
DDDXUB	104.129.12.238	5:45:36 PM	10/12/22
DDDXUB	45.249.94.56	2:36:58 PM	10/3/22

Fig 5. IT Admin Portal access records

The **same activity pattern** was identified on the **IT Admin Portal**, where the same user credentials were used to log in from the suspicious IP. The Admin Portal carries access rights that could allow **lateral movement**, **user management**, and **configuration changes**, which significantly raised the threat level of the incident.