Forensic Investigation on Widget Co.

Team – 09
Pramath Yaji
Faraz Ahmed
Phani Varun Munukuntla
Bhuvantej Ramachandra Reddy

To: Widget Co. Leadership and Security Teams

From: Team 09

Date: April 23, 2025

Subject: Forensic Investigation and Breach Analysis Report

Dear Widget Co. Leadership Team,

Thank you for the opportunity to assist Widget Co. with its cybersecurity investigation. Over the past few weeks, our team thoroughly examined your organization's October 2022 log data using Splunk for forensic analysis. Our investigation revealed a confirmed breach that originated from a phishing link and progressed through multiple attack phases, including MFA bypass, brute-force login attempts, and privilege escalation.

This report provides a detailed timeline of the attacker’s movements, forensic evidence, dashboards we developed for visibility, and specific remediation and policy recommendations targeted to both technical and leadership audiences. We are confident that our recommendations will help strengthen Widget Co.'s security posture and prevent similar incidents in the future.

We appreciate your trust in us and look forward to presenting our findings to the Leadership Team.

Sincerely,
Team 09

Table of Contents

1. Executive Summary

Widget Co. experienced a targeted cybersecurity breach during October 2022. The attack began with a successful phishing attempt involving user BDRVLS, who accessed a malicious domain (glasslu.com). This was followed by an MFA bypass, a brute-force attack on internal systems, and unauthorized access to the password vault. The attacker then leveraged stolen credentials (DDDXUB) to gain elevated access to critical systems including the Cloud and IT Admin Portal.

Using Splunk to analyze VPN, DNS, MFA, WidgetApp, and Password Vault logs, our team confirmed the timeline and scope of the breach. This report includes all indicators of compromise (IOCs), affected accounts, and associated IP addresses. Additionally, we created dashboards for incident visualization and monitoring and offer tailored security recommendations for immediate and long-term risk mitigation.

2. Methodology

We adopted a forensics-driven log analysis approach, leveraging Splunk for data ingestion, correlation, and anomaly detection. The datasets included 10 CSV files corresponding to sources such as VPN, Cloud, DNS, and MFA logs. We focused our attention on:

- Time-based anomaly detection (activity outside business hours)
- Correlation with known IOCs
- Repeated failed login attempts
- Access from unfamiliar geolocations
- Usage of privileged systems

Splunk enabled us to create dashboards that visually highlighted suspicious behaviour and provided quick insights for technical and non-technical stakeholders.

3. Findings and Breach Confirmation

Yes, a breach occurred. The following evidence supports this:

- 10/12 (Phishing Attack) – User BDRVLS clicked on a malicious link named **https://glasslu.com** which initiated the breach. We assume that the user provided their credentials which then was forwarded to the attacker.
- 10/12 (MFA Bypass) – There were multiple MFA bypasses from an interesting IP Address (180.76.54.93) which were logged for the user BDRVLS on key systems such as Billing.
- 10/12 (Brute Force Attack) – The attacker attempted brute-force logins into WidgetApp using BDRVLS credentials.
- 10/13 (Password Vault Access) – There was a successful login recorded from IP 180.76.54.93 using BDRVLS credentials. This was since there was no integrated MFA for Password Vault access.
- 10/14 (Phishing Attack) – The user TIIYAW was also phished since the subdomain of the domain **https://www.aeon.jp.co.glasslu.com** but this time we assumed that the user refrained from providing credentials as they understood that they were being phished.
- 10/14 & 10/24 – The attacker used the DDDXUB credentials which we assume, were stolen from the password vault and then gained unauthorised access through the password that was stolen to Cloud and IT admin Portal.

These events confirm there was a breach and the flow was phishing, credential compromise, MFA Bypass, Lateral movement and privilege escalation.

4. Dashboards

We created three main dashboards in Splunk:

- Dashboard 1: Reports that corelate with the breach are added in this dashboard. They provide value by laying out all the essential records associated with the breach.
- Dashboard 2: Here the reports are based on malicious activities, such as DNS, VPN, MFA etc. We were able to narrow down the exact malicious activity through these records.
- Dashboard 3: Here we created a few visualizations which helped us to come up with clear conclusions. It provided a better value with accessibility and readability.

5. Remediation Actions

- These two accounts were directly involved in the breach. BDRVLS was the original victim of the phishing attack and MFA bypass, while DDDXUB was later used by the attacker to access the Cloud and IT Admin Portal which suggests there was lateral movement and privilege escalation. Isolating both accounts prevents further misuse.
- Even though MFA was implemented, the logs shows that the attacker was able to bypass MFA. This suggests weak MFA configuration. Enforcing strict MFA means requiring MFA for all internal and external systems, including legacy systems. Also disabling fallback authentication methods like SMS or email codes which are more susceptible to social engineering.
- Enforce strict password policies where a user needs to change the password every 60 days to reduce the risk of long-term credential leaks and enforcing account lockout after 3 unsuccessful attempts.

- Attackers who gain access through phishing often deploy malware to maintain persistence. Machines used by BDRVLS, DDDXUB and any other device that accessed the malicious domains must undergo malware scanning and endpoint forensics.

6. Recommendations

I. IT/Security Team (Technical)

- Implement location-based access controls to block logins from regions where the company has no business presence. This reduces exposure to unauthorized access attempts from foreign IP addresses.
- Review current MFA implementation for bypass vulnerabilities and extend MFA to older or third-party applications that may not yet enforce it.
- Configure Splunk alerts to notify the security team immediately when accounts log in during non-working hours or when DNS/IP activity matches known Indicators of compromise.
- Integrate automated tools to regularly audit user access rights and enforce periodic password changes, ensuring compliance and reducing excessive privileges.

II. Leadership Team (Procedural)

- Regular simulated phishing exercises and security training will help employees recognize and avoid social engineering threats, reducing user-targeted attack success.
- Enhance the Incident response plan with specific steps for detecting and containing phishing based compromises and lateral attacker movement to improve future response efficiency.
- Investing in dedicated security personnel and EDR solutions ensures continuous monitoring and proactive threat hunting.
- Establish a quarterly review process to ensure that users only have the access they need which limits the privileges and reduces internal risk.

7. Conclusion

Our investigation confirms that Widget Co. was impacted by a multi-stage security breach originating from a phishing attack. The attacker successfully bypassed MFA and conducted a brute-force login, ultimately compromising privileged accounts and accessing critical infrastructure. The evidence points to a classic kill chain consisting of phishing, credential compromise, lateral movement, and privilege escalation.

Moving forward, Widget Co. must implement stricter MFA enforcement, enhanced alerting, periodic access reviews, and security awareness training. These changes, coupled with investment in dedicated security staff and EDR tools, will significantly reduce the likelihood and impact of future breaches. Our dashboards, forensic logs, and this report provide a foundation for strengthening Widget Co.’s cybersecurity resilience.

8. Appendix

DNS Activity by BDRVLS

Phishing

DNS Hit	Date	Machine Assignment	Time	date_hour	date_mday	date_minute	date_month	date_second	date_wday	date_year	date_zone	eventtype	host	index	linecount	punct	source	sourcetype
https://finance.yahoo.com	10/12/22	BDRVLS	5:18:14 PM	17	12	18	october	14	wednesday	2022	local		cdr-splunk	final_project	1	//.::_.,.://..	DNS.csv	csv
https://glasslu.com	10/12/22	BDRVLS	4:57:01 PM	16	12	57	october	1	wednesday	2022	local		cdr-splunk	final_project	1	//.::_.,.://.	DNS.csv	csv

Figure 1: DNS Activity by the user BDRVLS

BDRVLS MFA Activity

Bypass Method used by the attacker

Application	Authentication Method	Date	IP Address	Result	Time	Username	date_hour	date_mday	date_minute	date_month	date_second	date_wday	date_year	date_zone	eventtype	host	index	linecount	punct
Productivity Suite	Bypass	10/13/22	180.76.54.93	N/A	9:06:12 AM	BDRVLS	9	13	6	october	12	thursday	2022	local		cdr-splunk	final_project	1	//.::_.,.,_.,/.
Billing Software	Bypass	10/12/22	180.76.54.93	N/A	4:59:59 PM	BDRVLS	16	12	59	october	59	wednesday	2022	local		cdr-splunk	final_project	1	//.::_.,.,_.,/.
Productivity Suite	Bypass	10/6/22	70.107.95.217	N/A	1:04:48 PM	BDRVLS	13	6	4	october	48	thursday	2022	local		cdr-splunk	final_project	1	//.::_.,.,_.,/.
Billing Software	Bypass	10/3/22	70.107.95.217	N/A	3:28:48 PM	BDRVLS	15	3	28	october	48	monday	2022	local		cdr-splunk	final_project	1	//.::_.,.,_.,/.
Productivity Suite	Bypass	10/2/22	70.107.95.217	N/A	10:01:55 AM	BDRVLS	10	2	1	october	55	sunday	2022	local		cdr-splunk	final_project	1	//.::_.,.,_.,/.
Productivity Suite	Bypass	10/2/22	70.107.95.217	N/A	8:26:53 AM	BDRVLS	8	2	26	october	53	sunday	2022	local		cdr-splunk	final_project	1	//.::_.,.,_.,/.
Billing Software	Bypass	10/1/22	70.107.95.217	N/A	3:10:05 PM	BDRVLS	15	1	10	october	5	saturday	2022	local		cdr-splunk	final_project	1	//.::_.,.,_.,/.
Billing Software	Bypass	10/31/22	70.107.95.217	N/A	1:49:26 PM	BDRVLS	13	31	49	october	26	monday	2022	local		cdr-splunk	final_project	1	//.::_.,.,_.,/.
Widget Application	Bypass	10/28/22	70.107.95.217	N/A	9:20:10 AM	BDRVLS	9	28	20	october	10	friday	2022	local		cdr-splunk	final_project	1	//.::_.,.,_.,/.
Widget Application	Bypass	10/26/22	70.107.95.217	N/A	12:31:41 PM	BDRVLS	12	26	31	october	41	wednesday	2022	local		cdr-splunk	final_project	1	//.::_.,.,_.,/.

Figure 2: MFA Bypass by the attacker

WidgetApp Activity

Bruteforce attempt by the attacker

Auth	Date	IP_Add	Time	User	date_hour	date_mday	date_minute	date_month	date_second	date_wday	date_year	date_zone	eventtype	host	index	linecount
Fail	10/12/22	180.76.54.93	5:05:59 PM	BDRVLS	17	12	5	october	59	wednesday	2022	local		cdr-splunk	final_project	1
Fail	10/12/22	180.76.54.93	5:05:41 PM	BDRVLS	17	12	5	october	41	wednesday	2022	local		cdr-splunk	final_project	1
Fail	10/12/22	180.76.54.93	5:05:29 PM	BDRVLS	17	12	5	october	29	wednesday	2022	local		cdr-splunk	final_project	1
Fail	10/12/22	180.76.54.93	5:05:02 PM	BDRVLS	17	12	5	october	2	wednesday	2022	local		cdr-splunk	final_project	1
Fail	10/12/22	180.76.54.93	5:03:02 PM	BDRVLS	17	12	3	october	2	wednesday	2022	local		cdr-splunk	final_project	1
Fail	10/12/22	180.76.54.93	5:05:59 PM	BDRVLS	17	12	5	october	59	wednesday	2022	local		cdr-splunk	final_project	1
Fail	10/12/22	180.76.54.93	5:05:41 PM	BDRVLS	17	12	5	october	41	wednesday	2022	local		cdr-splunk	final_project	1
Fail	10/12/22	180.76.54.93	5:05:29 PM	BDRVLS	17	12	5	october	29	wednesday	2022	local		cdr-splunk	final_project	1
Fail	10/12/22	180.76.54.93	5:05:02 PM	BDRVLS	17	12	5	october	2	wednesday	2022	local		cdr-splunk	final_project	1
Fail	10/12/22	180.76.54.93	5:03:02 PM	BDRVLS	17	12	3	october	2	wednesday	2022	local		cdr-splunk	final_project	1

Figure 3: Brute force attempt by the attacker

Password Vault Activity

Attacker successfully authenticates himself

Authentication	Date	Src_IP	Time	Username	date_hour	date_mday	date_minute	date_month	date_second	date_wday	date_year	date_zone	eventtype	host	index
Success	10/13/22	180.76.54.93	9:05:09 AM	BDRVLS	9	13	5	october	9	thursday	2022	local		cdr-splunk	final_project

Figure 4: Successful authentication to password vault by the attacker

DDDXUB Activity

Attacker authenticates himself through DDDXUB user

Application	Authentication Method	Date	IP Address	Result	Time	Username	date_hour	date_mday	date_minute	date_month	date_second	date_wday	date_year	date_zone	eventtype
Cloud	Bypass	10/24/22	180.76.54.93	Pass	2:56:45 PM	DDDXUB	14	24	56	october	45	monday	2022	local	
IT Admin Portal	Bypass	10/24/22	180.76.54.93	Pass	2:48:06 PM	DDDXUB	14	24	48	october	6	monday	2022	local	
Cloud	Bypass	10/15/22	180.76.54.93	Pass	3:06:00 PM	DDDXUB	15	15	6	october	0	saturday	2022	local	
IT Admin Portal	Text	10/15/22	180.76.54.93	Pass	10:49:01 AM	DDDXUB	10	15	49	october	1	saturday	2022	local	

Figure 5: Attacker authenticates himself using DDDXUB account

Malicious DNS Activity

Associating DNS with IOCs

DNS Hit	Date	Machine Assignment	Time	date_hour	date_mday	date_minute	date_month	date_second	date_wday	date_year	date_zone	eventtype	host
https://lakeuthfreddie.buzz/xbalti%20v5%20+/	10/15/22	CYPFUK	2:00:58 PM	14	15	0	october	58	saturday	2022	local		cdr-splun
https://gregfurturt.buzz/doc/	10/15/22	SBVXFQ	8:51:22 AM	8	15	51	october	22	saturday	2022	local		cdr-splun
https://scottwayhigh.buzz/gb/adobe2020/	10/14/22	TCNCHM	11:42:43 AM	11	14	42	october	43	friday	2022	local		cdr-splun
https://www.aeon.jp.co.glasslu.com	10/14/22	TIIYAW	11:22:34 AM	11	14	22	october	34	friday	2022	local		cdr-splun
http://elitemaxx.online/elite.apk	10/14/22	RUDONQ	9:18:43 AM	9	14	18	october	43	friday	2022	local		cdr-splun
https://glasslu.com	10/12/22	BDRVLS	4:57:01 PM	16	12	57	october	1	wednesday	2022	local		cdr-splun
https://inemocharlieg.buzz/viewdocs/	10/12/22	TCNCHM	12:34:34 PM	12	12	34	october	34	wednesday	2022	local		cdr-splun
https://aeon.co.jp.xo176.com	10/11/22	DYHOPL	5:06:43 PM	17	11	6	october	43	tuesday	2022	local		cdr-splun
https://cliente-suporte2via.xyz	10/10/22	ECXYIM	11:03:50 AM	11	10	3	october	50	monday	2022	local		cdr-splun
https://payment-receipt.buzz/keybank.zip	10/8/22	PQCCZM	2:31:12 PM	14	8	31	october	12	saturday	2022	local		cdr-splun

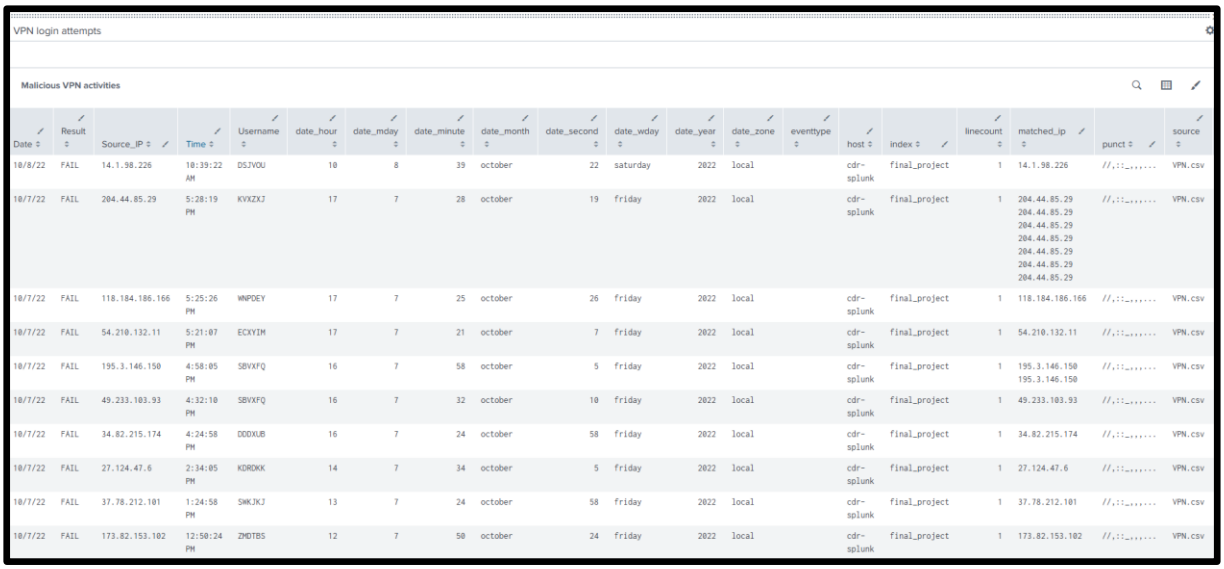
Figure 6: Analysing DNS with IOCs

Malicious IP

Associating IPs with MFA

Application	Authentication Method	Date	IP Address	Result	Time	Username	date_hour	date_mday	date_minute	date_month	date_second	date_wday	date_year	date_zone	eventtype
Productivity Suite	Bypass	10/13/22	180.76.54.93	N/A	9:06:12 AM	BDRVLS	9	13	6	october	12	thursday	2022	local	
Billing Software	Bypass	10/12/22	180.76.54.93	N/A	4:59:59 PM	BDRVLS	16	12	59	october	59	wednesday	2022	local	
Cloud	Bypass	10/24/22	180.76.54.93	Pass	2:56:45 PM	DDDXUB	14	24	56	october	45	monday	2022	local	
IT Admin Portal	Bypass	10/24/22	180.76.54.93	Pass	2:48:06 PM	DDDXUB	14	24	48	october	6	monday	2022	local	
Cloud	Bypass	10/15/22	180.76.54.93	Pass	3:06:00 PM	DDDXUB	15	15	6	october	0	saturday	2022	local	
IT Admin Portal	Text	10/15/22	180.76.54.93	Pass	10:49:01 AM	DDDXUB	10	15	49	october	1	saturday	2022	local	

Figure: 7 Associating IPs with MFA



VPN login attempts

Malicious VPN activities

Date	Result	Source_IP	Time	Username	date_hour	date_mday	date_minute	date_month	date_second	date_wday	date_year	date_zone	eventtype	host	index	linecount	matched_ip	punct	source
10/8/22	FAIL	14.1.98.226	10:39:22 AM	DSJVOU	10	8	39	october	22	saturday	2022	local		cdr-splunk	final_project	1	14.1.98.226	//,::_,,,...	VPN.csv
10/7/22	FAIL	204.44.85.29	5:28:19 PM	KVXZXJ	17	7	28	october	19	friday	2022	local		cdr-splunk	final_project	1	204.44.85.29 204.44.85.29 204.44.85.29 204.44.85.29 204.44.85.29 204.44.85.29 204.44.85.29	//,::_,,,...	VPN.csv
10/7/22	FAIL	118.184.186.166	5:25:26 PM	WNPDEY	17	7	25	october	26	friday	2022	local		cdr-splunk	final_project	1	118.184.186.166	//,::_,,,...	VPN.csv
10/7/22	FAIL	54.210.132.11	5:21:07 PM	ECXYIM	17	7	21	october	7	friday	2022	local		cdr-splunk	final_project	1	54.210.132.11	//,::_,,,...	VPN.csv
10/7/22	FAIL	195.3.146.150	4:58:05 PM	SBVXFQ	16	7	58	october	5	friday	2022	local		cdr-splunk	final_project	1	195.3.146.150 195.3.146.150	//,::_,,,...	VPN.csv
10/7/22	FAIL	49.233.103.93	4:32:10 PM	SBVXFQ	16	7	32	october	10	friday	2022	local		cdr-splunk	final_project	1	49.233.103.93	//,::_,,,...	VPN.csv
10/7/22	FAIL	34.82.215.174	4:24:58 PM	DDDXUB	16	7	24	october	58	friday	2022	local		cdr-splunk	final_project	1	34.82.215.174	//,::_,,,...	VPN.csv
10/7/22	FAIL	27.124.47.6	2:34:05 PM	KDRDKK	14	7	34	october	5	friday	2022	local		cdr-splunk	final_project	1	27.124.47.6	//,::_,,,...	VPN.csv
10/7/22	FAIL	37.78.212.101	1:24:58 PM	SMKJKJ	13	7	24	october	58	friday	2022	local		cdr-splunk	final_project	1	37.78.212.101	//,::_,,,...	VPN.csv
10/7/22	FAIL	173.82.153.102	12:50:24 PM	ZMDTBS	12	7	50	october	24	friday	2022	local		cdr-splunk	final_project	1	173.82.153.102	//,::_,,,...	VPN.csv

Figure 8: Malicious VPN activities

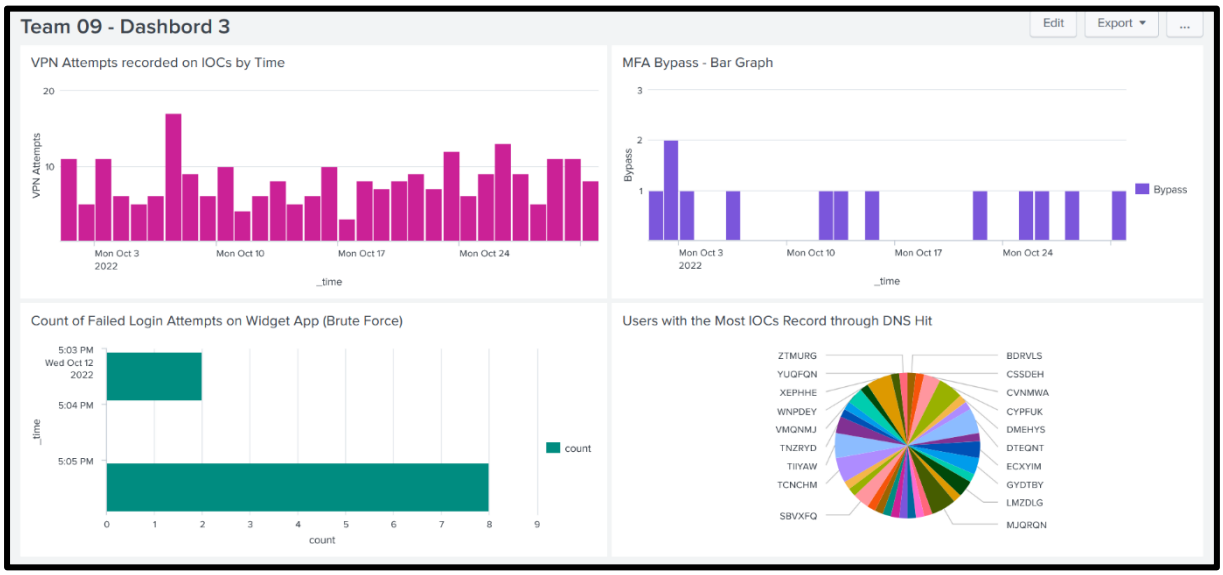


Figure 9: Visualization of appropriate activities tied with the breach