2025-02-06: Multiple forms of attack lead by phishing attack

## Date: 02/12/2025

## Handler: Sagarkumar Patel.

# Executive Summary

Between February 6th and 11th, 2025, we faced a coordinated series of cyberattacks on our system, SecureTech Solutions. The incident began when one of our employees inadvertently clicked on a phishing email containing a malicious link: **“****srv-61.kim.johnson.biz.”** This action compromised their account. From this compromised account, an unknown IP address **23.74.164.69(carrie64@ford.com)** sent out **79** phishing emails to our employees. Out of those, **7 employees**, including the initial victim, fell victim to the attack by clicking the link and submitting their credentials. Subsequently, these compromised accounts were used to launch multiple attacks involving multiple requests using DELETE, PUT, PATCH, TRACE, OPTIONS, HEAD, and other methods. These actions raised significant concerns regarding unauthorized resource manipulation, web reconnaissance, and possible command injection. Incident response includes identifying accounts that were compromised in phishing attacks, potential setups for exploiting the system, restoring the system from a clean backup, and implementing additional security controls to prevent further compromise. The estimated financial impact of the incident includes incident investigation, documentation, system downtime, and post-incident mitigation efforts.

# Background

# On February 12, 2025, the security team received reports from employees regarding what they believed to be a phishing message sent by an internal user. The incident began when one employee's account was compromised, leading to the sender sending phishing emails to other employees. Several employees interacted with the phishing site, which resulted in additional account compromises and various attacks being carried out.

# Credential-stealing and phishing attacks: Seven employees had their credentials stolen after clicking on the link “srv-61.kim.johnson.biz” and submitting their account information.

* Unauthorized resource manipulation: Many requests, including DELETE, PUT, PATCH, targeting end points on the server.
* Web reconnaissance or Probing: Many requests including TRACE, and HEAD, targeting mapping of the server and API structures.
* Potential command injection: Many requests, including PUT and PATCH methods to the endpoint, indicating upload of malicious payloads.

The security breach was confirmed through log monitoring and through forensic analysis of the mail.log and http.log.

# Timeline

2025-02-06 at 21:15:15: One of the employees with IP 10.10.1.7 clicked on the malicious link “srv-61.kim.johnson.biz” that was sent to them from 23.74.164.69(carrie64@ford.com) and submitted their credentials, which compromised their account.

2025-02-07 from 02:06 to 02:10: Attacker with 23.74.164.69 (carrie64@ford.com) used a compromised user account, which has IP 10.10.1.7, to send out 79 phishing emails to the internal employees containing the link “srv-61.kim.johnson.biz”.

2025-02-07 at 2:42: An employee with IP 10.10.3.185 interacted with the phishing email and submitted their credential to the link “srv-61.kim.johnson.biz,” compromising their account.

2025-02-07 at 4:51: An employee with IP 10.10.2.64 interacted with the phishing email and submitted their credential to the link “srv-61.kim.johnson.biz,” compromising their account.

2025-02-07 at 5:37: An employee with IP 10.10.1.234 interacted with the phishing email and submitted their credential to the link “srv-61.kim.johnson.biz,” compromising their account.

2025-02-07 at 6:05: An employee with IP 10.10.1.33 interacted with the phishing email and submitted their credential to the link “srv-61.kim.johnson.biz,” compromising their account.

2025-02-07 at 6:18: An employee with IP 10.10.1.198 interacted with the phishing email and submitted their credential to the link “srv-61.kim.johnson.biz,” compromising their account.

2025-02-07 at 6:59: An employee with IP 10.10.3.175 interacted with the phishing email and submitted their credential to the link “srv-61.kim.johnson.biz,” compromising their account.

2025-02-07 at 18:31: IP with 10.10.1.7 made DELETE and POST requests in list/list/categories and categories/search, potentially executing Resource tampering and content injection attacks.

2025-02-10 at 19:21: IP with 10.10.2.64 made a DELETE request to main/blog/app, indicating possible deleting or overwriting content structures.

2025-02-10 at 19:21: IP with 10.10.2.64 made a PUT request to tag/categories, indicating possible unauthorized updates or malicious tagging.

2025-02-11 at 19:17: same IP made TRACE request, indicating potential reconnaissance.

2025-02-09 at 15:59: IP with 10.10.3.175 made TRACE request on tags indicating testing for open proxies or misconfigurations.

2025-02-09 at 03:15 and 23:54: IP with 10.10.1.198 made PUT and HEAD requests to tag/tag/category and tags/blogs, which indicates data structure manipulation and recon.

2025-02-10 at 10:27 and 21:53: IP with 10.10.1.198 made PATCH and HEAD requests to wp-content and tags, which indicates data structure manipulation and recon.

2025-02-10/11: IP with 10.10.3.185 made a couple of TRACE and GET requests, potentially indicating reconnaissance/mapping attacks.

2025-02-11 at 00:22: IP with 10.10.1.234 made TRACE request on posts/categories indicating potential system discovery/diagnostics.

2025-02-10 at 20:42 IP with 10.10.1.33 made DELETE request to category/categories could be an indication of system structures removed, potentially leading to destructive actions.

2025-02-11 at 10:05: IP with 10.10.1.33 made PUT request to blog/category/categories indicating potential file injection.

# Findings

1. Several employee accounts from SecureTech appear to be compromised. It began with one employee clicking on a phishing email, which resulted in their account being compromised. This led to the compromised account sending additional phishing emails within the company, ultimately affecting six more accounts, for a total of seven compromised accounts.
2. After the accounts were compromised, the attacker used methods like DELETE, PATCH, PUT, and TRACE on URLs that usually don’t get touched by regular employees. This includes things like:

* tags/categories
* main/blog/app
* wp-content/tags
* category/categories
* tag/tag/category

1. One suspicious method was TRACE, which can be used to see how servers respond — attackers often use this to look for weaknesses or misconfigurations.
2. The PATCH and PUT requests seemed aimed at editing or uploading stuff to the site — maybe trying to change content or exploit something in the system (like a plugin or a backend script).
3. We also saw DELETE requests going to pages that seem like they could be part of a content management system. That could mean someone was trying to remove data or mess with the site structure.
4. Some POST requests looked like they were being used for more than just logging in — maybe to send or change data in a sneaky way.
5. The same types of strange behavior were seen across multiple accounts, which could mean either that the attacker had access to many credentials or moved through the system after getting in once.

# Actions Taken

• **2025-02-12 at 09:00AM:** Logs were collected from HTTP traffic after an employee reported the phishing email from another employee to identify unusual or unauthorized user behavior from employee accounts.

• **2025-02-12 at 10:15 AM:** A set of internal SecureTech accounts, all seven of them, were flagged for performing suspicious actions not typically part of their role, such as PATCH, PUT, DELETE, and TRACE requests to admin-like URLs.

• **2025-02-12 at 11:00 AM:** Investigation started to determine whether these actions were malicious or part of the employees’ legitimate tasks. The behavior was compared to logs from normal employees, and clear differences were observed.

• **2025-02-12 at 01:30 PM:** A decision was made to temporarily suspend login access to the compromised accounts to prevent further misuse while the incident was reviewed.

• **2025-02-12 at 02:00 PM:** The affected accounts were forced to reset passwords and enrolled in mandatory **Multi-Factor Authentication (MFA)** to secure future access.

• **2025-02-12 at 03:15 PM:** Web server access logs were preserved and backed up for forensic analysis. A review of firewall and WAF (Web Application Firewall) settings was initiated.

• **2025-02-12 at 04:30 PM:** Updated WAF rules to detect and block risky HTTP methods (e.g., TRACE, DELETE, PATCH) unless explicitly required by the application.

• **2025-02-12 at 05:00 PM:** Internal IDS (like Snort or Suricata) was configured to monitor traffic from internal employee IPs and raise alerts for abnormal web method usage.

• **2025-02-13 at 08:00 AM:** Educated SecureTech employees through an internal security briefing about phishing risks, credential reuse, and unusual access patterns.

• **2025-02-13 at 09:15 AM:** Scheduled full plugin review and CMS update for any services running internally, to patch vulnerabilities that attackers might exploit next.

# Financial Impact

|  |  |
| --- | --- |
| Item | Cost |
| Incident investigation (security team) 3 team member \*5 hours @ $50/hr | $750.00 |
| Documentation & reporting (2 Analyst) 4 hours @ 45/hr | $360.00 |
| Affected System Downtime ( 6 hours \* $700/hr productivity value) | $4,200.00 |
| Post-incident Mitigation Efforts ( Path, audit, WAF config, and plugin reviews) | $600.00 |
| Total | $5,910 |

1. Team of 3 security experts looked at the log for 5 hours with a 50/hr wage = $750.
2. We had 2 incident writers working on it for 4 hours with a 45/hr wage = $360
3. Due to system downtime, we lost revenue from customer subscriptions and ads for 6 hours at a rate of $700/hr, totaling $4,200.
4. After the incident, we configured many security tools in order to investigate and monitor, which cost = $600.

# Lessons Learned

## Successes

 **Log Review Led to Behavior-Based Insights**  
By comparing suspicious activity to patterns from known normal employee behavior, we were able to confidently distinguish between benign user actions and potential threats. This approach minimized false alarms and sharpened our response accuracy.

 **User Role Awareness Helped Contextualize Actions**  
Knowing that all compromised accounts belonged to SecureTech employees helped prevent mislabeling internal activities as attacks. This showed the importance of correlating identity and access roles with log data.

 **Suspicious Commands Flagged Without Automation**  
The team manually identified several risky HTTP method patterns (e.g., PATCH, TRACE, CONNECT) without relying solely on automated tools. This hands-on review demonstrated that human intuition remains a key layer of security defense.

 **Multi-User Log Cross-Check Validated Findings**  
Logs were not only checked for isolated events but also cross-referenced among users to detect repetition of attack-like behavior. This technique made it easier to detect coordinated or repeated patterns that a single log entry might not reveal.

 **Flexible Thinking During Investigation**  
The assumption that all abnormal behavior equals an attack was challenged through deeper analysis, proving that investigative flexibility leads to more accurate conclusions. This helped the team avoid overreacting while still taking precautionary steps.

## Opportunities for Improvement

|  |  |  |
| --- | --- | --- |
| Issue | Recommendation | Action Item Owner |
| Inconsistent detection of unusual HTTP methods used by internal users | Implement application-layer controls that flag or restrict advanced HTTP methods unless explicitly required for job function. | IT Security Team |
| Lack of context-aware behavioral monitoring for employee accounts | Deploy User and Entity Behavior Analytics (UEBA) tools to establish behavioral baselines and detect deviations. | SOC (Security Operations Center) |
| Overly broad web access from internal accounts to unknown external domains | Apply domain reputation filtering and restrict access to only vetted, job-relevant external resources. | Network Administrator |
| No formal classification of internal user access levels for web application functions | Introduce tiered access roles (e.g., standard, power user, admin) with associated permissions and limit web-layer capabilities accordingly. | HR & IT Policy Committee |
| No defined response protocol for employee-originated suspicious network behavior | Create an internal incident response playbook specific to employee misuse or compromise. Include escalation tiers for repeated policy violations. | Incident Response Lead |