**Memo Title:**   
**Vulnerability To Phishing Attacks Increased Following CrowdStrike Catastrophic Update.**  
  
**Executive Summary:**  
  
The cybersecurity company CrowdStrike has recently pushed a software update causing widespread crashes[1]. The cybersecurity company CrowdStrike accounts for up to 14% of the security software market by revenue [1]. With such widespread market penetration by CrowdStrike, it is therefore likely that one of our users or vendors has CrowdStrike software installed, has suffered an outage, and therefore may be searching for fixes – making themselves vulnerable to phishing attacks purporting to recover data lost during the outage. We must immediately move to close off vectors of attack to prevent further losses.   
  
**Introduction:**

On July 19, 2024 CrowdStrike pushed a content update for the CrowdStrike Falcon sensor, this update was faulty however and caused 8.5 million devices running Microsoft Windows to crash unable to restart [2]. The widespread nature of this sudden catastrophic system failure was quickly pounced upon as a source of Phishing attacks masquerading as a solution to this problem[3]. A Zip archive named crowdstrike-hotfix.zip poses as a utility to recover content lost during the downtime caused by CrowdStrike’s update, however CrowdStrike notes in a blog post that this utility is in fact the Remcos malware which enables remote access to administrator permissions by an outside actor, log keystrokes, and capture screenshots, audio, and clipboard contents of infected systems [3][4].

**The Threat:**

This threat is malware that is the result of phishing attacks. It spreads by the user opening messages or downloading files purporting to be a fix to recover files lost in the crash from the recent Crowdstrike Update. This threat is currently relevant because we are in the period immediately following the Crowdstrike update where many users are impacted. It is expected that the issues caused by the Crowdstrike update may take many weeks to fix – as the I.T. team will need to reimage each computer manually [1]. During this period where users are expecting messages from I.T, where I.T. is too busy to respond to user requests, and where users may believe themselves to be impacted due to the widespread nature of the outage, technically inexperienced users may be susceptible to messages that promise to recover lost files, or the users may seek out solutions themselves.   
  
If the user does open the Remcos malware, the nature of the malware means that it may be able to automatically execute regardless of user account controls since it can operate through user’s opening Microsoft documents with embedded macros [5].  
  
  
  
This threat primarily targets the user domain as it is an attack based on social manipulation. Failure to preemptively act during this period may result in malware granting external access being installed on devices throughout the company – thus exposing the company to potential data breaches as well as ransomware attacks. This vulnerability may not just come from our own company, but from vendor software.

**Remediation Steps:  
1.) Implement Spam Filtering To Prevent First-Stage Attacks:** Phishing primarily operates through manipulating social targets, all external emails should be labeled as external, and marked as suspicious if they include any embedded links or documents. Enabling filters should take less than one hour, or below $250.00. Doing nothing will increase the likelihood of phishing attacks, it may be possible that none occur – however if we could rely upon the technical skills of our employees it is unlikely that we would have IT employees to begin with.   
  
**2.)** **Seize All Corporate Windows Computers That Have CrowdStrike Installed:** The original CrowdStrike outage can occasionally be fixed during a restart in the instance where the computer is able to fetch an update before the CrowdStrike bug causes the system to crash [6]. This means there are computers that have suffered an outage but may not have reported an issue to I.T. These users are more vulnerable to social engineering regarding recovering files as they still have functional devices that may have lost files in the outage. Seizing these computers will allow I.T. to get to these devices before the phishing attack does. Additionally, taking these computers will allow I.T. to switch to a separate security vendor than CrowdStrike following the outage. It should be noted that these computers need seized anyway due to the outage requiring reimaging.  
  
This fix will require around 1 hour per machine, or around 250.00 per device. Depending on the severity of the impact this may mean it will take around $250.00 per employee assuming each employee has one device.   
  
Doing nothing means that computers impacted by the CrowdStrike update that have not restarted will never operate again until they are reimaged. This means that every employee who relies upon their computer to complete their tasks will be entirely useless, and will be paid to effectively do nothing. This means that every technologically dependent employee and any employees who depend on them are deadweight until their computer is fixed.   
  
Doing nothing in regards to operational computers means risking phishing attacks on employees who have lost files due to the outage and are thus vulnerable.

**3.) Disable Office Macros** – If our users are not technically sophisticated enough to recognize a phishing scam, they are not technically sophisticated enough to operate Microsoft Office Macros. Disabling macros will disable a vector of attack[5]. This should take less than one hour at around $250.00 total to change system wide setting.

Failure to act may mean that office macros will be an attack vector in the future.

**4.) Disable Automatic Updates** – If a cybersecurity company like CrowdStrike can push bad updates that crash computers, then vendors infected by malware can too, it may would be prudent for us to disable updates until they are verified by our cybersecurity team that the updates do not cause problems. This may increase the cost for updates as each update will have to be manually reviewed. This could cost as much as $250.00 per week as it will take 1 hour each week to review all updates.   
  
  
**Conclusion:**

Vulnerability to phishing attacks promising fixes to losses caused by outages has increased following the CrowdStrike induced outage. We must immediately take action to disable vectors of attack to prevent further losses.   
  
**REFERENCES:**  
[1] Lily Hay Newman Matt Burgess Andy Greenberg. “How One Bad Crowdstrike Update Crashed the World’s Computers.” *Wired*, Conde Nast, 19 July 2024, www.wired.com/story/crowdstrike-outage-update-windows/.

[2]Weston, David. “Helping Our Customers through the CrowdStrike Outage.” *The Official Microsoft Blog*, 20 July 2024, blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/.

[3]Operations, Counter Adversary. “Likely eCrime Actor Capitalizing on Falcon Sensor Issues: Crowdstrike.” *Crowdstrike.Com*, 20 July 2024, www.crowdstrike.com/blog/likely-ecrime-actor-capitalizing-on-falcon-sensor-issues/.   
  
[4]Michali. “Remcos Malware.” *Check Point Software*, Check Point Software, 20 Sept. 2022, www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/remcos-malware/.

[5]“What Is Remcos Malware?” *What Is Remcos Malware?*, www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/remcos. Accessed 22 July 2024.   
[6] Andrew Cunningham    -    Jul 19, 2024 3:43 pm UTC. “Crowdstrike Fixes Start at ‘Reboot up to 15 Times’ and Get More Complex from There.” *Ars Technica*, 19 July 2024, arstechnica.com/information-technology/2024/07/crowdstrike-fixes-start-at-reboot-up-to-15-times-and-get-more-complex-from-there/.