CYBERMINUTE
Alberta Cybersecurity Insights

TLP: CLEAR ○○○

Faulty CrowdStrike Update Leads to Mass Outages and a Spike in Phishing

On 19 July 2024, cybersecurity company CrowdStrike released a faulty update for their Extended Detection and Response (XDR) tool, Falcon, leading to worldwide outages impacting multiple sectors. The update caused affected devices to either suffer a boot loop or a Blue Screen of Death (BSOD), which severely disrupted flights, emergency services, healthcare, transactions, schools, and many other businesses. 8.5 million Windows systems were confirmed to be affected, but the total impacted systems are likely to be higher as the confirmed devices were only the ones with crash dump sharing enabled.

Remediation for the failure was provided in due course. CrowdStrike fixed the cause of the issue and provided guidance to individually recover systems. Microsoft had released a custom recovery tool (WinPE) to expedite the removal of the faulty component. However, threat actors had already begun opportunistically taking advantage of this desperate situation.

On the same day as the outage, multiple attacks were delivered through phishing emails and typo squatting domains, leveraging the situation to lure victims into interacting with malicious links and attachments. The threat actors responsible for launching these attacks masqueraded as either technical support offering guidance and patches or competing companies offering alternative products.

One of the most notable attacks involved the use of newly registered domains to distribute a malicious ZIP folder masquerading as a legitimate fix for the faulty CrowdStrike sensor and led to the deployment of a remote access trojan. Another attack used a Word document which masqueraded as recovery instructions and contained a malicious macro. When the macro was executed, a payload was retrieved from an attacker-controlled URL that led to the deployment of an infostealer.

The CrowdStrike outage indirectly generated a notably high spike in maliciously created domains. One researcher identified close to 200 impersonating domains within one week of the incident. Another researcher identified over 3000 CrowdStrike themed domains had been registered since the incident. This large volume can present a difficult challenge for security teams to defend against.

At times of major news stories, teams can enhance their security posture with the use of protective DNS tools. These tools can leverage domain reputation databases and threat intelligence feeds, as well as detect domains that have been quickly established at a high volume by a Domain Generation Algorithm (DGA). Any enhanced measures can be temporary and should be reviewed promptly to limit the risk of creating false-positive blocks.

Click Here to Read More!

Increase in Publicly Exploited Ransomware

Ransomware attacks, where malicious actors encrypt a victim's data and demand a ransom

Global Cyber-Attack Trends: Q2 2024

Per a recently released report from Check Point, the second quarter of 2024 has for its release, have become increasingly sophisticated and prevalent. Globally, the frequency of these attacks has risen by approximately 9% in the second quarter of 2024 compared to the previous quarter. This uptick is part of a larger pattern observed, with cybercriminals targeting a wider range of sectors, including healthcare, manufacturing, and technology. According to a recent Zscaler report, the energy sector has seen almost a 530% increase in ransomware targeting between April 2023 and April 2024.

Alberta has not been immune to these increases, with both public and private organizations in the province having been targeted, reflecting the broader global trend. With Alberta contributing heavily to the energy, manufacturing, and technology sectors, it is somewhat understandable how the province may be experiencing a spike in ransomware. However, several other factors are also contributing to this rise. Firstly, the proliferation of ransomware-as-a-service (RaaS) platforms has lowered the barrier to entry for cybercriminals. These platforms allow even those with limited technical skills to launch effective ransomware attacks. Additionally, the increasing digitization of services and the shift towards remote work have expanded the attack surface for cybercriminals, making it easier for them to exploit vulnerabilities.
witnessed a significant escalation in cyber threats. There has been a staggering 30 per cent year-over-year increase in global cyber-attacks, averaging 1,636 attacks per tracked organization per week. This alarming rise is attributed to the continued digital transformation across industries, the sophistication of cybercriminals leveraging advanced techniques, and the economic motivations behind ransomware and phishing attacks. Geopolitical tensions and supply chain vulnerabilities have further exacerbated the situation.

The Education sector, which includes research work, was noted as the most impacted sector, experiencing a staggering 53 per cent increase in cyber incidents when compared to the same period last year. The Government sector, including the military, and Healthcare sectors were the second and third most impacted groups during the second quarter of 2024, with 2,084 and 1,999 attacks per week respectively. The trend towards targeting these sectors underscores the need for robust cybersecurity measures, especially in sectors handling sensitive information and have traditionally been underprepared for such sophisticated threats.

Globally, Latin America, Africa, and Europe have seen the largest increases in cyber-

The provincial government and cybersecurity experts are responding to this threat with increased vigilance. Efforts include enhancing cybersecurity frameworks, promoting awareness campaigns, and encouraging organizations to adopt robust security measures. However, the evolving nature of ransomware means that staying ahead of attackers remains a constant challenge.

The rise in ransomware attacks in Alberta in 2024 underscores the urgent need for comprehensive cybersecurity strategies. As cybercriminals continue to adapt and innovate, it is crucial for both public and private sectors to collaborate and fortify their defenses against this persistent threat.

Click Here to Read More!

attacks, with Africa recording the highest volume of incidents per organization, nearing almost 3,000 attacks per organization per week. Closer to home, North America is shown to account for the majority—58 per cent—of the publicly extorted ransomware attacks during the second quarter. Per the report, the bulk of these published instances of ransomware were in the Manufacturing sector—highlighting it as a particularly vulnerable target—with the sector experiencing a 56 per cent year-over-year increase in such attacks.

The surge in cyber-attacks highlights the need to re-evaluate current cybersecurity strategies. Organizations must prioritize robust security measures to protect against the growing sophistication of cybercriminals who are leveraging advanced techniques such as AI and machine learning. Heightened vigilance and improved cybersecurity protocols are a necessity in the modern world, particularly in the most targeted industries.

Click Here to Read More!