AON

Crowdstrike / Windows Event Briefing

Implications for Cyber Re/Insurers: Initial Findings

July 21, 2024

Key Takeaways

- CrowdStrike, a global cybersecurity firm, released an update for its Falcon sensor which caused system crashes on Microsoft Windows systems globally.
- Airline, financial, and health services were some of the industries impacted by the outage.
- Cyber insurance portfolios containing system failure coverage for these industries and others may see claims, however the extent to which this is a covered event for insureds will vary.
- This event highlights the interconnected nature of software ecosystems, and presents an industry learning opportunity to reassess approaches to addressing portfolio accumulation risk.

Contents

Background / Disclaimer

This note is intended for clients of Aon's Reinsurance Solutions. Please also refer to Aon's Better Decisions Brief and Cyber Solutions blog tracking this event with a focus on Commercial Risks.

This alert describes a quickly changing situation. The information contained herein is based on publicly available information believed to be accurate at the time of publishing, Aon has not verified such information independently, and cannot guarantee the accuracy, adequacy, completeness of such information. Aon accepts no liability for any loss incurred in any way whatsoever by any person who may rely on it, and any recipient shall be entirely responsible for the use to which it puts this information. The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity and we recommend seeking appropriate professional advice to address a specific situation.

Event Overview

Background

CrowdStrike, based in Austin, Texas, is a global cybersecurity firm founded in 2011, and according to the company's website has almost a dozen security and IT tools, is involved with about 300 of the Fortune 500 companies, six out of the top 10 health care providers, eight of the top 10 financial services firm, and eight of the top 10 technology firms. CrowdStrike has an advanced cloud-native platform for protecting endpoints, cloud workloads, identities and data. The CrowdStrike Falcon platform leverages real-time indicators of attack, threat intelligence on evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities – all through a single, lightweight agent.

What Happened

On July 19, 2024, at 04:09 UTC CrowdStrike released a sensor configuration update for Falcon to Windows systems. The configuration update triggered a logic error resulting in a system crash and blue screen (BSOD (blue screen of death)) on impacted Microsoft Windows systems. By July 19, 2024, at 05:27 UTC the sensor configuration update was remediated. CrowdStrike customers who were online between the times referenced and using Falcon sensor for Windows version 7.11 could be impacted. Systems that had automatically downloaded the updated configuration between the times referenced were susceptible to a system crash. The sensor configuration update does not affect Linux or MacOS.

Per CrowdStrike's blog on the outage, configuration files are referred to as "Channel Files" and are part of the behavioral protection mechanisms used by Falcon sensor. Updates to the Channel Files are routine and occur several times per day in response to novel tactics, techniques and procedures discovered by CrowdStrike. Each channel is assigned a number as a unique identifier, "c-00000291-", it has a .sys extension but is not a kernel driver. Channel 291 controls how Falcon evaluates named pipe execution on Windows systems. Named pipes are used for normal, inter-process or intersystem communication in Windows. The update at 04:09 UTC was to target newly observed, malicious named pipes being used by common C2 (Command and Control) frameworks.

The configuration update caused a logic error that resulted in the operating system crashing. The Channel file "C-00000291*.sys" with timestamp of 04:09 UTC is the problematic version and the Channel file "C-00000291*.sys" with timestamp of 05:27 UTC or later is the reverted (good) version.

Impact

Microsoft has estimated 8.5 million Windows devices have been affected. The broad economic and societal impacts reflect the use of CrowdStrike by enterprises that run many critical services.

The air travel industry had more than 3,000 flights cancelled and a reported 23,900 flights delayed due to ticketing, operations, other services, at airports. The healthcare industry was impacted by the outage. In the US some emergency call centers in were impacted by the outage. Healthcare providers had services disrupted, such as elective hospital procedures, procedures that required anesthesia, and medical visits were cancelled or paused. In the UK, the number used to call for emergency ambulances wasn't impacted but across health provider offices there were problems with the appointment and patient record system used across the health service.

The financial industry was also impacted. In the US, some banks reported login issues, and trades on the stock exchange were delayed because bankers couldn't access their work systems. In the UK news updates about the exchange couldn't be published but the exchange itself was operational. In South America customers of a bank may have had issues accessing digital services due to the outage and services being unstable during that time.

Aon's Threat Intelligence Analysis

This incident highlights how interconnected and dependent companies across the globe are and how an error (in this case) can impact business operations. Vendors should have processes and procedures in place when updating software. This should encompass how the update is developed, tested on development systems, monitored to watch for any adverse effects of the update, and then pushed out to production systems. How that process works for a security vendor pushing updates multiple times per day without any issues will be something to watch going forward. Companies should assess any third and fourth-party exposure they have to this incident. Even if your organization was not impacted or has been remediated, there may be external parties your organization relies on which remain effected. Understanding those relationships is important. Companies should have a proactive plan for gaining visibility across the supply chain in addition to considering scenarios that may impact operational resilience of the supply chain.

It is strongly recommended that insureds follow the guidelines from CrowdStrike and Microsoft to remediate system crashes or system unavailability due to the outage.

Re/Insurance Implications

Key implications for cyber re/insurance

- This is reported to be a non-malicious event, meaning that "system failure" coverage, where offered, within cyber re/insurance policies is the relevant loss trigger
- Business interruption (loss of income and extra expenses incurred), where offered due to system failure, is expected to be the most directly affected head of damage, subject to applicable waiting periods
- Dependent business interruption, data restoration, incident response and voluntary shutdown costs may also be applicable and contribute to re/insured losses
- At the individual risk level, Aon expects this event to trigger greater attention to system failure coverage grants and business interruption waiting periods
- At the portfolio level, Aon sees this event as an opportunity for the market to react by improving granularity on codifying policy information important for understanding portfolio accumulation risks stemming from certain coverage grants, to allow more nuanced event loss estimation and accumulation scenario analysis.
- The industry has developed specific re/insurance and bond products which this event will test, both from an event definition and loss quantum perspective.

Insurance coverage focus

System Failure: Aon has analyzed several leading cyber insurance wordings and found there are a range of approaches to offering coverage triggered by "system failure" or "non-malicious" events such as this. Some leading carriers offer this as part of their standard form, whereas others do not.

We understand that deviation from standard forms is common, for example to regularly add system failure triggered coverage as an endorsement, or conversely to restrict coverage on risks and industries of particular concern e.g. airlines, which in this event and in previous system failure events incur massive costs immediately when systems are down.

Business interruption waiting periods: A "time deductible" is typically applicable to business interruption losses in cyber policies. Standard time deductibles typically range between 8-12 hours but these can be as low as 6 hours or as high as 24 hours as these are negotiated on a case by case basis.

Loss of income and extra expenses: Business interruption coverage typically covers the loss of income and extra expenses sustained during the period of interruption until restoration, after any applicable waiting period. While some companies and industries may immediately incur costs (e.g. airlines) or immediately lose revenue to competitors (e.g. online retailers), for other companies there may no such immediate revenue loss due to the nature of their revenue streams (they may experience briefly delayed revenue rather than lost revenue), and where manual workarounds can be applied.

Dependent business interruption: Additional to the expected "primary" impact on business interruption cover, insureds who are dependent on another business who has experienced the outage may have suffered downstream or contingent impact on their ability to generate income or extra expenses e.g. clients of any affected Managed Software Service Providers ("MSSPs").

Portfolio Accumulation

This is likely to be the most important cyber accumulation loss event since NotPetya in 2017. However, the overall loss quantum is currently uncertain and will primarily depend on:

1. The prevalence of coverage for system failure, which varies across the market, and
2. The duration until successful manual remediation at each affected insured, versus the applicable waiting periods on their cyber policies

This event brings into focus the need for greater transparency of system failure coverage grants, waiting periods and in general a more granular approach to tracking coverage items relevant for monitoring aggregations at portfolio level. For example, distinguishing between coverage, limits and waiting periods for each of business interruption as follows:

<u>Business interruption coverage grant subsets:</u>
Security failure – own IT
System failure – own IT
Dependent security failure – IT providers (named vs unnamed)
Dependent system failure – IT providers (named vs unnamed)
Dependent security failure – non-IT providers (named vs unnamed)
Dependent system failure – non-IT providers (named vs unnamed)

Event definitions

Specific coverage for events with widespread impact such as this is a developing area of the cyber market, featuring in a subset of original policies, reinsurance treaties and catastrophe bonds. This event will bring into focus:

1) the wording aspect of these products / covers e.g. “are non-malicious events covered?” and
2) the threshold aspect: does the event “qualify” as an event of required magnitude and will the attachment points of cover be reached?

Contact Information

To talk to Aon's Reinsurance Solutions about this event, please contact a colleague on our cyber leadership team.

Rory Egan
Head of Cyber Analytics, UK Product Leader
rory.egan@aon.com

Alex Podmore
Senior Cyber Broker - UK
alex.podmore@aon.com

Jack Hammond
Senior Cyber Broker - UK
jack.w.hammond@aon.com

Benedict Davey
Senior Cyber Broker - UK
benedict.davey@aon.com

David Grigg
US Head of Cyber
david.grigg@aon.com

Crystal Boch
US Head of Cyber Analytics
crystal.l.boch@aon.com

Vlad Polyakov
Senior Cyber Broker - UK
vlad.polyakov@aon.com

Paul Preston
Senior Cyber Broker - US
paul.preston@aon.com

Cyber Threat Intelligence

Paula Mendez
Associate Director
paula.mendez@aon.com

About Aon:
Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Our colleagues provide our clients in over 120 countries and sovereignties with advice and solutions that give them the clarity and confidence to make better decisions to protect and grow their business.

Follow Aon on LinkedIn, Twitter, Facebook and Instagram. Stay up-to-date by visiting the Aon Newsroom and sign up for News Alerts here.