Q2

Q2 customers,

As part of our ongoing communications strategy, we wanted to provide a thorough update following last week's SolarWinds cyber-incident. First, I want to reiterate that Q2 does not use any SolarWinds Orion Platform products. I also want to describe the concrete actions we've taken as part of our commitment to ensuring Q2's hosting environments are safe and secure.

MITRE ATT&CK

In 2020, Q2 implemented MITRE ATT&CK – a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. It's used as a foundation for developing specific threat models and methodologies in the cybersecurity community and brings communities together to develop more effective response capabilities. Q2 uses MITRE ATT&CK as part of its tool selection process, connecting the actual security operations, threat discovery, and incident response in real-world activities. The Cybersecurity and Infrastructure Security Agency (CISA) now reports in the ATT&CK framework, making it easier to match nomenclature. Specifically, this helped Q2 during the SolarWinds issue - Alert (AA20-352A) - Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations.

Endpoint detection and remediation

While Q2 doesn’t use SolarWinds Orion products, our robust security posture includes tools and processes that helped reduce the risk around the SolarWinds attack. Q2 uses an Endpoint Detection and Remediation (EDR) solution that places an autonomous learning agent on each endpoint (server/laptop). This agent learns what normal behavior for the endpoint is – then if it begins to act differently, the agent alerts, and the system isolates the asset from the network. Q2 also utilizes the EDR vendor’s Enhanced Response Service, which monitors all system alerts and supports Q2’s team as we investigate issues identified by the EDR tool. We are confident this particularly advanced tool would have alerted us to any abnormal activity connected with this compromise, wherein the malware lay dormant and undetected after being installed, then activated days later.

Outbound connections lockdown

Q2 also locks down all outbound connections to ‘known domains,’ meaning if an endpoint attempts to reach out to a new domain, it would be blocked. In order to connect to a ‘previously unknown domain’, Q2’s security team must manually review and approve the connection. In the SolarWinds compromise, the malware attempts to reach out to a foreign ‘command and control’ server – to notify the bad actors that a successful deployment has occurred and then to receive further instructions. If the malware cannot connect to that remote server, an important attack angle is removed.

Other protections

I’ve written several Q2 blogs, LinkedIn entries, and articles around Q2’s egress defense, zero-trust network design, robust endpoint security, and Secure Access Service Edge (SASE). In addition, read how we leverage blockchain and encoding to position data as part of Q2’s security.

Third-party review

Since the SolarWinds attack, we’ve investigated our networks, assets, and suppliers, using third parties to assist in the review of our work and validate our findings. No evidence of compromise has been found.

We will continue to review and document Q2’s third-parties responses related to the incident as required by our Third-Party Risk Management Program.

Thank you for your continued partnership. I wish you and your families a wonderful holiday season and peace and good health in 2021.

Lou Senko
Chief Availability Officer, Q2