Perspecta's approach to addressing advanced persistent threats

Key highlights

- Top recipient of Defense Advanced Research Projects Agency (DARPA) funding for cybersecurity research
- Perspecta's approach to the SolarWinds supply chain cyberattack
- Securing the Navy Marine Corps Intranet (NMCI), the largest intranet in the world, successfully detecting more than 300 million threats and preventing more than 2.5 billion unauthorized intrusion attempts per year
- NATO Communications and Information Agency (NCIA) utilizes Perspecta's Cyber Defense Situational Awareness (CDSA) services to gain situational awareness across the NATO classified environment
- Currently supporting cybersecurity operations and support for DHS and major agencies within DOD

The supply chain compromise of specific versions of SolarWinds Orion resulted in widespread nation-state cyberattacks against U.S. federal, state and local government agencies and technology companies.

Perspecta is working with numerous customers and partners, analyzing the security breaches caused by the exploit within certain versions of SolarWinds Orion and applying CISA directed guidance to affected customer environments.

Our solution

Due to the sophistication of the SolarWinds exploit and evidence of other associated cyber threat activity, Perspecta's approach is a multifaceted action plan focused on reaction, remediation and response.

Reaction

Perspecta is available to provide advisory services as well as consulting engagements to customers on immediate actions to reduce risk from the SolarWinds attack. This includes:

- Enterprise-wide action plans for stopgap measures to potential SUNBURST and SUPERNOVA backdoors created as a result of compromises found in specific versions of SolarWinds Orion using guidelines as directed by CISA
- Vendor updates to recommended industry best practices and frameworks to deploy countermeasures within your network security infrastructure
- Providing key reactionary steps including host blocking, account management, encryption settings and security policy definition and settings within your enterprise to reduce the risk from any additional exploits that may have been created as a result of the compromised SolarWinds Orion software

Remediation

While initial reactive steps are important, the length of exposure to the SolarWinds Orion exploit may require a closer examination of the enterprise to identify other backdoors that may have been created within the environment. Some key areas where Perspecta can assist are:

- Compromise assessments with Perspecta pen-testing teams
- Network security and compute infrastructure inspection for tampering
- Gap analysis, OS and system memory forensics and alternative tools recommendations for customers who are looking to restore functionality, but are not looking to utilize SolarWinds for the foreseeable future

Response

If there are clear indicators that the enterprise has been compromised at multiple levels, Perspecta can provide a full suite of services to proactively assist the customer in exploring all long-term response options. We deliver:

- Deep experience in building defense in depth network architectures that utilize multivendor network security components
- Significant expertise in messaging to deploy enterprise-class email as a service
- Application services to provide a code inspection of the application in question
- Application services to inspect a customer's source code, build tools and infrastructure and convert the environment to a true DevSecOps continuous integration and continuous delivery pipeline with policy-based automation to enforce security best practices and controls
- Application modernization / acceleration to the cloud that can essentially eradicate any existing backdoor and malware embedded in current legacy code

Contact us

contactus@perspecta.com
14295 Park Meadow Drive
Chantilly, Virginia 20151

perspecta