Threat Image

Entering may, we hear about drought-stricken Spain and climate changes in Europe. Climate change and cybersecurity are two topics that likely seem unrelated, but there are a number of reasons why industry professionals need to pay attention to this existential threat. According to Chloe Messdaghi, CEO & Founder of Global Secure Partners, the link is "complex and multifaceted". She argues that climate change is leading to more opportunities for cyber-threat actors to strike. These opportunities include extreme weather events that can compromise digital systems and disrupt internet connectivity, new green technologies that are vulnerable to attacks and geopolitical instability caused by rising temperatures that lead to cyberwarfare between rival nations. (1)

In late March, the company 3CX was hit by a supply chain attack. This might be the first example of a **double** supply chain attack; a software supply chain attack leading to another software supply chain attack. The company 3CX provides enterprise software for communication including chat, video calls, and voice calls. According to Mandiant, the initial breach was via malicious software downloaded from Trading Technologies website. 3CX software for Windows and macOS was then injected with a backdoor. Software updates, including this backdoor, were then automatically distributed to 3CX's customers. The attack appears to be financially motivated, and North Korean-sponsored actors are suspected to be behind the incident. (2) It's now been confirmed there were other victims related to the same attack. According to cybersecurity company Symantec, there are two critical infrastructure organizations in the energy sector among the victims, one in the U.S. and the other in Europe. In addition to this, two other organizations involved in financial trading were also breached. (3)

Threat actors have been abusing macros in Microsoft Word and Excel documents for years to download and install malware on Windows devices. After Microsoft finally disabled macros by default in Word and Excel Office documents, threat actors began turning to other less commonly used file formats to distribute malware. Since mid-December, threat actors has used Microsoft OneNote attachments. this is not only a theoretical problem. Security researchers have found that they ultimately led to a ransomware attack on a compromised network. (4) These days OneNote is making an important change, by blocking the opening of embedded files with a dangerous extension. (5)

Latest Cyberthreats and Advisories (6)

- NCSC, FBI and Other Security Agencies Publish Smart City Guidance
- Protecting the 2024 Election Is CISA's Top Priority
- Black Basta Ransomware Gang Claims Yellow Pages Canada Breach
- Climate Change Will Exacerbate Cyberthreats
- 1.4 Million Members Impacted by American Bar Association Breach
- More Victims Emerge in 3CX Supply Chain Attack

(1) https://www.infosecurity-magazine.com/news/climate-change-cyber-risks
(2) https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise
(3) https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/xtrader-3cx-supply-chain
(4) https://www.bleepingcomputer.com/news/security/how-to-prevent-microsoft-onenote-files-from-infecting-windows-with-malware/
(5) https://www.securityweek.com/microsoft-onenote-starts-blocking-dangerous-file-extensions/
(6) https://blog.isc2.org/