Fighting cyberweapons built by private businesses

blogs.microsoft.com/on-the-issues/2021/07/15/cyberweapons-cybersecurity-sourgum-malware/

July 15, 2021

A world where private sector companies manufacture and sell cyberweapons is more dangerous for consumers, businesses of all sizes and governments. We take this threat seriously and have disrupted the use of certain cyberweapons manufactured and sold by a group we call Sourgum. The weapons disabled were being used in precision attacks targeting more than 100 victims around the world including politicians, human rights activists, journalists, academics, embassy workers and political dissidents. To limit these attacks, we focused on two actions. First, we built protections into our products against the unique malware Sourgum created, and we shared those protections with the security community. Second, we issued a software update that will protect Windows customers from exploits Sourgum was using to help deliver its malware. We've undertaken this work in close collaboration with the Citizen Lab at the University of Toronto's Munk School.

We believe Sourgum is an Israel-based private sector offensive actor or PSOA. Citizen Lab has identified the group as a company called Candiru. Sourgum generally sells cyberweapons that enable its customers, often government agencies around the world, to hack into their targets' computers, phones, network infrastructure and internet-connected devices. These agencies then choose who to target and run the actual operations themselves.

We initially started this work after receiving a tip from Citizen Lab about malware used by Sourgum. The Microsoft Threat Intelligence Center (MSTIC) and Microsoft Security Response Center (MSRC) spent weeks examining the malware, documenting how it works

and building protections that can detect and neutralize it. We named the malware DevilsTongue. We've built protections against DevilsTongue into our security products, and we've shared these protections with others in the security community so they can protect their customers. Technical information for customers and the security community is available here.

By examining how Sourgum's customers were delivering DevilsTongue to victim computers, we saw they were doing so through a chain of exploits that impacted popular browsers and our Windows operating system. Earlier this week, we released updates that, when installed, protect Windows customers from two key Sourgum exploits.

These attacks have largely targeted consumer accounts, indicating Sourgum's customers were pursuing particular individuals. The protections we issued this week will prevent Sourgum's tools from working on computers that are already infected and prevent new infections on updated computers and those running Microsoft Defender Antivirus as well as those using Microsoft Defender for Endpoint.

This is part of broader legal, technical and advocacy work we're undertaking to address the dangers caused when PSOAs build and sell weapons. As we've previously said, these companies increase the risk that weapons fall into the wrong hands and threaten human rights. That's why, for example, we filed an amicus brief in a legal case brought by WhatsApp against another PSOA called NSO Group.

As we increase our work to identify PSOAs and disrupt the capabilities of their weapons, we will continue to identify them using the names given to trees and shrubs, as we've done with Sourgum. This is similar to how we use elements of the periodic table to name nation-state actor groups we have identified.

We're grateful to Citizen Lab for sharing the malware that sparked this work and for its offer to work with potential victims of these attacks.

Tags: cyberattacks, cybersecurity, Microsoft Defender, Microsoft Threat Intelligence Center, MSRC