Microsoft weighs revamping flaw disclosures after suspected leak

April 28 2021, by Kartikay Mehrotra, Bloomberg News

Credit: Pixabay/CC0 Public Domain

Microsoft Corp. may revise a program that shares coding flaws in its products with other companies after a suspected leak led to a sprawling cyber-attack against thousands of Microsoft Exchange email clients globally.

The technology giant is weighing how and when to share data with at least some of the 81 participants in the Microsoft Active Protections Program, according to six people familiar with it including existing members who sought anonymity citing a Microsoft non-disclosure agreement. The others requested anonymity because they aren't authorized to discuss the matter publicly.

MAPP grants some customers information about vulnerabilities in Microsoft's products and services days or weeks ahead of public disclosure. It is widely regarded by participants as a critical data-sharing tool to defend against potential attacks.

However, Microsoft fears MAPP participants may have tipped off hackers after the company shared a critical vulnerability with its top tier of members around Feb. 18, according to four people familiar with Microsoft's investigation into the cause of the attack. Microsoft publicly released software updates to patch the problem on March 2.

The company's inquiry has focused on at least two Chinese companies as possible sources of the leak, according to the people familiar with the probe. Four MAPP participants told Bloomberg News they'd recently disclosed detailed logs of network activity to Microsoft since the Exchange attack. In some cases, companies volunteered the data unprompted, while in others Microsoft requested additional data. The companies asked to remain anonymous, citing their non-disclosure agreement with Microsoft.

Microsoft's vulnerability disclosure in late February was followed by one of the most efficient, wide-ranging cyber-attacks in history. Microsoft has blamed state-sponsored Chinese hackers, dubbed Hafnium, for the attack which compromised more than 60,000 government, corporate and private email systems around the world, much of which occurred over the last weekend in February.

Microsoft declined to comment on potential changes to MAPP, nor would the company discuss its MAPP disclosures in February or possible leaks by participants. The company said it remained committed to the program and its wide-ranging list of members from the U.S., Israel, Russia, China, Japan, Australia, India and parts of Europe.

"We believe there are many benefits to mutual information sharing with the security community to help protect our mutual customers against attacks," the company said in a statement. "We continue to evaluate how to best balance the benefits of this sharing with the risk of early disclosures."

In response to queries from Bloomberg News, China's Ministry of Foreign Affairs stated, "China resolutely opposes any form of online attacks or infiltration. This is our clear and consistent stance. Relevant Chinese laws on data collection and handling clearly safeguards data security and strongly oppose cyber-attacks and other criminal activity."

China has proposed a global security standard which it says is "for the benefit of international digital governance" and urged others to work with it to safeguard global data security. "We hope the media adopts a professional and responsible attitude, relying on comprehensive evidence when determining the nature of cyberspace events, but not groundless speculation," according to the ministry's statement.

Until MAPP was created, both criminal hackers and computer researchers would wait for Microsoft to disclose patches on the second Tuesday of every month, known as "Patch Tuesday." The two camps would then race to reverse engineer the patches in hopes of identifying the root vulnerability, which attackers could then exploit and defenders would attempt to protect against, according to Microsoft.

Patch Tuesday still exists. MAPP was started in 2008 to give some of

Microsoft's biggest customers a head start against the criminals.

At least 13 Chinese companies have participated. Two of them have been removed. Hangzhou DPtech Technologies Co. was kicked out in 2012 for breaching its non-disclosure agreement, according to Microsoft. A cybersecurity researcher found that Hangzhou had leaked evidence of a critical vulnerability in a Microsoft product to Chinese hackers.

Last year, Qihoo 360 Technology Co. was removed after being the target of U.S. imposed export controls due to national security concerns, according to three people familiar with the matter. A year earlier, Microsoft named Qihoo 360, Tencent Holdings Ltd. and Palo Alto Networks Inc. as the top contributors to MAPP.

Hangzhou DPTech didn't respond to questions about their removal from MAPP. Qihoo declined to comment.

MAPP is organized into three tiers: entry-level, advance notification and validation. Members of the validation group—mostly virus-detection firms—are invited to receive vulnerabilities sometimes weeks ahead of public disclosure. Some of the details shared with MAPP participants are subject to a non-disclosure agreement.

Microsoft may elect to re-shuffle members of the top tier, according to three people familiar with options being considered by the company. The Microsoft Security Response Center, which runs MAPP, may also simply reassess how much critical intelligence they share with companies considered close to certain nations, including China, according to the people.

Microsoft could also embed a unique test in pieces of its code, known as a watermark, that serve as sort of digital bread crumbs in the event of a

leak. It's unclear if watermarks were used in the data distributed to MAPP participants in February, but Microsoft has previously used them and could reintroduce them in the future, according to one of the people.

Microsoft requires MAPP participants to share data and vulnerabilities the same way it discloses the bugs in its products. Multiple MAPP participants told Bloomberg News that Microsoft's requests for information have surged in recent years but especially in the months since the Exchange and SolarWinds cyber-attacks. In the latter instance, which was publicly disclosed in December, Russian hackers infiltrated at least nine U.S. agencies and 100-private-sector companies after installing malicious code in software updates for Texas-based SolarWinds Corp.

But there are risks for Microsoft. Many of the companies on the MAPP list are presumed to have at least informal ties with the state security apparatus in their country of domicile, meaning Microsoft's vulnerability disclosures may be shared with governments with some frequency, said one former MAPP member who asked not to be identified because of an NDA.

Microsoft is unlikely to remove any Chinese participants despite the possible Exchange leak, according to two people familiar with the MAPP review. But the company could limit how much data it shares with members in China, the people said. A Chinese cybersecurity law requires corporations to provide access to their technology and assist with investigations involving crime and national security.

If Microsoft were to eliminate MAPP participants in countries not politically aligned with the U.S., the company would handcuff part of its own intelligence operation.

"While there are risks in partnering with Iranian, North Korean, Russian or Chinese companies, Microsoft also uses the program to its

advantage," said Chester Wisniewski, a principal research scientist at the cybersecurity firm Sophos.

Microsoft President and Chief Legal Officer Brad Smith said in January 2020 that the company generates about 2% of its global sales from China, or about $2.86 billion that year. The potential to enhance that revenue could motivate the company's disclosure policies, said Robert Potter, chief executive officer of Internet 2.0, a cybersecurity firm which advises the U.S. and Australian governments.

"Like all large companies Microsoft has to balance maintaining market access inside of China and security considerations," Potter said. "Over time, this balance is getting harder to maintain and this introduces risks to other customers. The pressure is making that decision more binary.