MSI Ransomware Attack: What Can Be Learned

Zevin Alifi

University of Advancing Technology

May 13, 2023

On April 7th of 2023, hardware manufacturer MSI was subject to an attack on their information systems that will compromise the integrity of their firmware for some time. Due to how recent the attack was as of this writing, as well as MSI's lack of transparency, the nature of the attack is at least partially speculative. What we know officially is that the breach includes source code for the software and signing keys for the software, meaning it will be incredibly easy for malicious actors to spoof official MSI firmware. Data that was previously confidential has also been made public after the incident.

MSI's course of action was to remain mostly silent on the issue, their official statement does not communicate what was stolen, how it occurred, the attackers identities or even motivations. They did not even clarify if customer data was hit in the attack or not. *"Upon detecting network anomalies, the information department promptly activated relevant defense mechanisms and carried out recovery measures " MSI Global (2023, April 7).* It could be that they do not wish to draw attention to the issue or give the attackers attention, but there is troubling implications with how little is explained officially on the matter. Especially since we later find out that the attack could create complications with MSI's relationship with intel, given that their own software was leaked in the attack as well. At the very least, MSI did urge it's users to only update their firmware or BIOS from the official source.

Given MSI's silence on the matter, the primary source of information about the attack comes from sources outside of MSI, particularly the attacker group themselves, a group that goes by the name

of “Money Message”. They purport that they acquired the confidential company data through a ransomware attack perpetrated by themselves where the data was acquired and encrypted on MSI’s systems, and they demanded a payment of 4,000,000 from the company to get access to it back and unleaked. When MSI failed to produce the ransom, that is when they undisclosed more information about the attack.

That leaves the question of what could have been done to mitigate or prevent the damage from occurring. Ransomware usually requires an incentive to install in order to be effective. It always attempts to disguise itself as legitimate software. So, policies should be put in place for team members to not install software without authentication from higher-ups. In order to reduce how compromised the organization is in the event of a ransomware attack, offline backups of the important data should be set up and maintained. At the very least, this will ensure that the attackers have little ransom to work with, as you can get your data back on your own network after it is secure, no payment required.

Ransomware is designed to be very easy to detect after the fact, that is, of course, how the attackers expect to create a profit. The victim has to be aware that their important data is encrypted and no longer accessible, and if a ransomware attacker did their job thoroughly, your organization’s online backups should be compromised as well. This should also mean that you are being contacted by the attacker, either directly or through the program that they used to perform the attack. This much is intuitively obvious, but by this point the damage has already been done.

However in instances of human operated ransomware, certain activity can be intelligently determined to be set up by the attacker preparing to launch a ransomware attack. Sophisticated attackers will attempt to gain an understanding of the network after they have been granted access, which can leave a trail provided you have good network monitoring tools. If the issue is appropriately responded to fast enough, you may even be able to mitigate how much of the data is compromised or in a best case scenario, deny the attacker access to everything.

Monitoring the network at this time can reveal symptoms of an attempt at ransomware. For instance, increased disk activity can suggest that a disproportionate amount of data is being encrypted at once. Sudden creation of new accounts could suggest that the attacker is trying to brute force a login with escalated privileges to allow them to access and modify data. Port scans coming from within your network is also an indication of malicious activity. An attacker with an understanding of your backups will also attempt to interface with them. Several failed attempts at accessing a shared drive could be brute force attempts to intercept online backup solutions.

Unauthorized installations of certain software is also a big indicator of potential ransomware. If a team member's device has software that is not approved or recognized, it could easily be a tool to initiate the ransomware attack. *"The presence of MimiKatz, Process Explorer, PC Hunter, or other hacking tools is a dead giveaway you're under attack."* ITPro Today (2022, April 20). The machines on the network behaving in atypical ways can be a signifier too. If a device was previously performing reasonably before, but is now under performing, it could mean that an attempt to encrypt organization data is currently under way and the computer's resources are being utilized to do this.

MSI Global (2023, April 7). - the leading brand in high-end Gaming & Professional Creation. MSI. (n.d.). https://www.msi.com/news/detail/MSI-Statement-141688

Fadilpašić, S. (2023, May 8). *The MSI data breach might have leaked some very important intel code*. TechRadar. https://www.techradar.com/news/the-msi-data-breach-might-have-leaked-some-very-important-intel-code

Toulas, B. (2023, April 6). *Money message ransomware gang claims MSI breach, demands $4 million*. BleepingComputer. https://www.bleepingcomputer.com/news/security/money-message-ransomware-gang-claims-msi-breach-demands-4-million/

ITPro Today (2022, April 20). *How to spot the warning signs of ransomware attacks*. ITPro Today: IT News, How-Tos, Trends, Case Studies, Career Tips, More. https://www.itprotoday.com/vulnerabilities-and-threats/how-spot-warning-signs-ransomware-attacks