Malware Attacks: Lessons Learned from an Emergency Communications Center

Background

In 2019, a regional emergency communications center (ECC) experienced a malware attack impacting operations. A telecommunicator was using the internet to search for the address of a known suspect for law enforcement and clicked on a link that downloaded a virus to the machine.

This document highlights the impacts, response, long-term recovery, and the lessons learned from this center's experience with a malware attack.

Malware, short for "malicious software," includes any software (such as a virus, Trojan, or spyware) that is installed on your computer or mobile device. The software is then used, usually covertly, to compromise the integrity of your device. Most commonly, malware is designed to give attackers access to your infected computer. That access may allow others to monitor and control your online activity or steal your personal information or other sensitive data.[1]

Impacts

The worm began immediately damaging the operating system and system files on the originating machine, while simultaneously searching for similar internet protocol (IP) addresses to connect to other machines. The worm was found on over 33 machines, including three computer-aided dispatch (CAD) consoles. Most of the impacted machines were used for training and administrative functions. In total, the attack occurred over the span of about eight hours.

Response

On the morning of the malware attack, a telecommunicator reported that their computer was locking-up and not responding to the on-duty supervisor. The ECC director and the agency's information technology (IT) department were notified that a computer on the ECC floor was experiencing issues.

- Initially, they believed it was only a single computer; however, when the agency's IT department was notified about a second computer experiencing similar issues, they realized the computers might be infected with a worm.
- Once IT was made aware of the possibility of a worm, staff began quickly disconnecting computers from the network to prevent further damage.
- IT department staff extracted the disk drives from the impacted machine and inserted them into another machine to run antivirus software.
- The IT staff used tools to ascertain what was happening within the network. Worms were extracting network data and sending it to an IP address in another country.

[1] CISA.gov, *Malware Tip Card*, last accessed September 21, 2021.

1hr

The ECC attempted to keep the CAD system running; however, within an hour of the attack, they disconnected field personnel because of the remote nature of those operations. ECC staff verbally notified field personnel of the situation and provided regular updates until their computers were safe to use.

- In addition to notifying field personnel, the ECC notified surrounding agencies of the malware attack and provided regular updates on the situation.

Long-Term Recovery

Due to the damage, each computer had to be completely wiped clean and rebuilt. It took the agency approximately one month to return to pre-event status, with all of the machines in operation. Prior to this event, the ECC performed daily back-ups of their data but did not perform daily back-ups of the operating system. They had to pay their vendors to reinstall all the software after the attack. Thankfully, the ECC has two subnets for their operations. The worm was only able to locate one subnet so the other was ultimately not impacted.

Following the cyberattack, the ECC coordinated with their cybersecurity insurance provider to discuss appropriate coverage. The ECC is currently navigating increased deductibles and considering the liabilities and risks associated with operating an ECC.

Lessons Learned

Ensure operating systems and data are backed-up regularly to assist in a speedy recovery

ECCs/public safety answering points (PSAPs) should frequently back-up their data and operating systems.[2] Accessible, up-to-date information and systems can improve recovery times by making it easier for agencies to rebuild their systems. Staff should know how to reinstall operating systems from backup data and should have access to a schedule of items to bring back online following an attack.[3] ECCs/PSAPs should also back-up data and operating systems on a secure secondary drive, stored offline, for further separation. ECCs/PSAPs should periodically test their ability to restore systems from back-ups.

Ensure networks are separated and critical operations are on a closed network

ECCs/PSAPs should segment their networks to protect against complete loss of operations during an attack. ECCs/PSAPs should also place machines with internet access on a separate network from critical operations.

Educate staff on cyber threats and how to prevent them

Staff are often the first users to notice operating issues or recognize differences in equipment function. ECCs/PSAPs should consider implementing cybersecurity training to help educate staff on cybersecurity threats and best practices to help prevent cyberattacks.

---

[2] CISA.gov, *Cyber Essentials Toolkit*, last accessed October 19, 2021.
[3] Ibid.

Implement strong password protocols and two-factor authentication

ECCs/PSAPs should review policies for password requirements to ensure users and staff use strong, non-duplicative passwords, and non-generic usernames to minimize the risk of intrusion. Additionally, ECCs/PSAPs should consider implementing two-factor authentication to provide an added layer of security, as possible.

Identify staff with knowledge of system and network architecture

ECCs/PSAPs should be familiar with their systems and network architecture. Designated staff members should be available during cyberattacks to identify points of ingress and egress, connection and disconnection points, and any vulnerabilities. ECCs/PSAPs should develop an architectural diagram of their network, as it is a helpful resource to have available for staff and external partners who may be assisting in the response. The diagram should be updated as needed and considered in succession planning.

Coordinate with service providers when developing and updating cyber response and vulnerability plans

ECCs/PSAPs should engage with their service providers to ensure the providers follow the cyber practices set forth by each agency, as well as industry best practices. It is recommended that ECCs/PSAPs review and document any external service providers that have access to their network. ECCs/PSAPs should consider limiting access to their network and permit service providers access on an as-needed basis.

Disable the use of universal serial bus (USB) ports

ECCs/PSAPs should consider disabling the use of USB ports for CAD, records management systems, or any other mission critical systems. USB devices (e.g., USB sticks, thumb drives, and smartphones) may contain viruses. Connecting infected USB devices to a USB port can have devastating effects on ECC/PSAP operations.[4]

For more information on this and other cybersecurity initiatives, contact ng911wg@cisa.dhs.gov or visit cisa.gov/safecom/next-generation-911 and cisa.gov/communications-resiliency.

[4] CISA.gov, *Protect Your Center from Ransomware*, last accessed October 15, 2021.