Securing Endpoints

Protecting a New Frontier in Cyber Warfare

Edited by **MOHAN DAS VISWAM**

Perimeter has long been a preferred war zone for the adversaries and defenders of the cyber space. No more. The long battle has ensured that technologies have become mature enough to make it extremely difficult and costly for adversaries to attack and successfully breach a properly protected perimeter. It has led to the shifting of action to users' devices like desktops, laptops, tablets and mobile phones. So, endpoints have become a new frontier in Cyber Warfare.

The endpoints in government / public sector ecosystem are mostly autonomous housing sensitive data which needs to be strictly compartmentalized. Typically, there is no single authority which should have access to all of users' data even within a single department or organization. This makes securing these endpoints extremely challenging as most of advanced enterprise endpoint security solutions are designed to transfer control of endpoints from users to technical experts called administrators which is not a desirable model for this ecosystem. So, in this article, we will try to formulate a set of best practices to secure autonomous endpoints by relying on a combination of less intrusive technologies and greater emphasis on user cyber hygiene.

Importance

The security of the endpoints, especially the autonomous ones, is the primary responsibility of the user of that endpoint. IT support will ensure that the perimeter, the local network and the data centers are well protected but a compromised endpoint can undermine all the security measures outside of the endpoint. So, the security of the endpoint is equally important, if not more, than the security of the environment. The tricky part is that the users of endpoints are typically normal people and not cyber security experts which makes protecting the endpoints even more challenging. It also brings us to the most important and ignored component of the security chain viz. education, training and sensitization of users of these endpoints. In order to understand the importance of the fact, let us think about the latest and deadliest agent of our times – Coronavirus. The best way to protect oneself from Coronavirus disease, as highlighted by almost all the health experts of the world, is PREVENTION and it involves the most basic hygiene principles taught to us since pre-school viz. keep hands clean, wash them regularly, sneeze or cough with face covered, etc. Coronavirus has reaffirmed that strict adherence to the basic hygiene can protect us even from the most dangerous of adversaries. The same principle holds good for cyber security as it does for health security. If the endpoint and the data stored in it is an integral part of our life, then it is our responsibility to follow the basic cyber security hygiene principles proposed in this article like we do for our health and prevent compromise as 'Prevention is better than cure.'

Although prevention reduces the chances of compromise to a large extent, it does not guarantee 100% safety. Even after strict adherence to the best practices, there can be some persistent and well-resourced adversaries which may be able to compromise the endpoints. It means that though prevention should be our focus, we must also plan for minimizing loss and speed-up recovery in case of a compromise also called MITIGATION. In this article, we will also try to frame some basic mitigation principles like first-aid for cyber compromise.

Prevention Principles

Prevention requires actions from both technical architects as well as end users. In this article, we will focus on actions to be taken by end users for the sake of simplicity and clarity. The following principles can help end users use their endpoints safely and securely,

Syed Hasan Mahmood
Scientist-C
hasan@nic.in

- **Compartmentalize:** Today each individual who is working is typically assigned a device. The devices are no longer shared. User's device is her/his responsibility along with the data stored on it. Same is true for personal devices. The data sensitivity is different for official and personal devices so is the security architecture of the devices. Hence, in order to prevent cross contamination and inadvertent data leak/ loss, it is recommended to use official devices for carrying out official business and personal devices for personal business. It is also advisable to use as few devices as possible as it is easier to manage and secure.
- **Say 'No' to Pirated Software:** Free copies of expensive software are almost irresistible to users. They seem to be a product of goodness of humanity almost too good to be true. But as an old adage goes, there are no free lunches in this world. The 'free' copies are actually not free. They charge by compromising the endpoint, giving its control to the attacker and loss of data with the user being oblivious to it. Hence, it is recommended to use genuine operating support and software with patching support to ensure latest security updates for the operating system. DO NOT use pirated software as they are generally laced with malware.
- **Adopt FOSS:** There is a class of software created out of sheer goodness of human nature called Free and Opensource Software (FOSS). The developers create the software and dedicate them to the community for free use, development and maintenance. These can be used as is or customized based on the needs of individual users. The motivation for FOSS is enhancement of human knowledge and use of this knowledge for the better of one and all. The most common and powerful example of a FOSS is the Linux kernel which drives the world ICT today. The users are recommended to look out for opensource alternative of the software they need as they are available in plenty today. Their source code is freely available to anyone who wishes to verify it, hence chances of malicious code in them are quite low compared to a closed-source software.
- **Avoid PUA:** As more and more software / apps are installed on a device, the codebase installed on the device increases and along with it its attack surface. More the number of lines of code running on a device more are the chances of some of them being weak or vulnerable. Vulnerable code makes it much easier for attackers to compromise the device and take control. So, it is recommended to install software which are regularly used and remove all Potentially Unwanted Applications (PUA) from the device. Also, remove software which are not regularly used after their use to reduce the attack surface.
- **Update, Update, Update:** Updating or patching the installed software / apps is the single most potent tool in the lay users quiver to ward of the resourced adversaries. Imagine a security hole already present in a software but not known to anyone. The software is safe for now as the hole is not known to anyone. As soon as a fix for that hole is released by the software provider everyone knows about the hole. Now the same software becomes extremely unsafe as the world knows about the security hole and it can easily be exploited to compromise the device. So, updating the software as soon as the patch is released is not a luxury but a necessity.
- **Endpoint Security Agent:** Just like an external sentinel is important to guard a physical premises, a third-party virtual sentinel is essential to maintain the security of user devices. Any good endpoint security agent like an antivirus, endpoint detection & response (EDR), etc. must be installed on the user devices to protect the device from adversaries. It is recommended to install a good endpoint security agent, keep it updated and running at all times.
- **Least Privilege:** Need-to-know is an established principle of information secrecy. Least privilege is an extension of the same principle. It means that each user should be given access / privileges based on her / his need. This principle helps in minimizing damage if an account / access is compromised. It can be used as following: Create two accounts in Windows viz. user with administrator privileges (admin) and user without administrative privileges (user). Use user account for daily access and admin account only when needed to install software or make system level changes.
- **External Attachments:** External attachments like USB drive, portable disks, CD/DVD disks, etc. are exploited rigorously to infect and compromise devices. Once an external storage disk is attached to a compromised device, it is infected and when an infected disk is attached to other devices, they can also get infected. Thus, creating a chain of infection. So, it is recommended to avoid using unknown removable drives like portable hard disks, pen drives, etc. as far as possible. However, if absolutely needed, scan it thoroughly using antivirus program before using.
- **PowerShell:** PowerShell in Windows devices exposes the command-line administrative console for making system altering changes. Attackers frequently use this console to compromise devices by means of automated scripts. Normal users typically never use PowerShell for any of their activities. Hence, it is recommended to disable PowerShell to make is harder for attackers to compromise Windows devices.
- **Remote Desktop:** Remote Desktop is a powerful feature which helps users access their devices from other devices by opening a virtual connection to their devices. It is especially useful when users have to access data stored on their devices when physically away from their devices. But lately this functionality is actively used by attackers to compromise devices and take control by means of weak passwords or vulnerabilities in RDP protocol. So, it is recommended to disable Remote Desktop on Windows machine at all times. In order to address the data portability requirements, users are advised to use cloud storages to make their data accessible anytime from anywhere.
- **Remote Support:** IT support teams rely heavily on free Remote Support tools like TeamViewer, Ammy Admin, Anydesk, etc. to provide support to users on their end devices. These tools keep the agent running on user devices at all times. These tools are actively used to compromise and take control of the user device by means of weak passwords or vulnerability in these tools by the attackers. So, it is requested to avoid using them as far as possible. However, if absolutely necessary, then use it in run-mode only without installing it and terminate it after use. If it does not allow run-mode and has to be installed then uninstall it immediately after use.
- **Password Managers:** Passwords are a necessary evil in most of the IT systems today. Though multiple alternatives are being invented to remove the use of memorized passwords but they are still not pervasive and passwords are here with us for some more time. Most of our current password policy owes its allegiance to the guidelines for creating safe online passwords in NIST SP 800-63 released in 2003 by Bill Burr. Ironically, after making users suffer with passwords for 15 years, Bill has admitted that he was wrong. "Much of what I did I now regret", he says. Traditional password policies like long and complex passwords, mandatory password change, not allowing copy-paste passwords etc. actually reduces security around passwords. Multiple researches have shown that these policies force users to choose predictable passwords based on patterns and reuse them at multiple places in order to make it easier to memorize and reproduce. Once the password pattern is guessed by attackers, they can predict passwords with ease. Also, reusing passwords can be dangerous as compromise of one website / system will reveal passwords for many others. So, it is recommended to use zero-entropy password managers like masterpassword to have strong & unique passwords for each account. DO NOT re-use passwords for different accounts. DO NOT share passwords or other account details. Change password immediately if shared with someone or at the slightest hint of compromise.
- **Unlocked & Unattended:** Unlocked and unattended devices can be potentially dangerous especially in presence of a mole

in the premises. The attacker with the help of an insider can bypass traditional security checks and install malicious code on the device to compromise and take control. Also, compromised insiders can steal data through USB disks from unlocked and unattended devices. So, it is recommended to NOT leave your machines unlocked and unattended at any time.

- **Unknown Links & Files:** Users have to be very careful about the hyperlinks to click and files to download while browsing the Internet or emails. Attackers typically place malicious code within attractive hyperlink / file, taking about an impossible sale or opportunity. As soon as the users click on that link / file, the malicious code gets downloaded and executed on the user device thus compromising the device and taking its control. So, it is recommended to be very cautious before clicking on links or downloading files in unsolicited emails or attractive websites and avoid them completely as far as possible.
- **Official Email:** Free email services make users agree to a declaration that the data in your mail boxes can be accessed by them for various purposes. Some even go to the extent making users agree, inadvertently, to the declaration that the data in the mail boxes are public information and can be used for targeted advertising by multiple parties and shared with governments of host countries. Putting sensitive or critical official data on private email servers can lead to data loss / leak. The users sharing official data over non-gov email can be prosecuted for the loss / leak of data under various sections of the Indian Penal Code (IPC). So, it is mandatory for users to only use official email address (@gov.in, @nic.in) for official communications.
- **Data Backup:** Data has become one of the most essential assets for organizations and individuals alike. Unfortunately, it is also very fragile. Sometimes even slight mishandling or media holding the data can render it useless and users helpless. Infection of devices can also impact the availability of data as attackers can encrypt or delete it after taking control as in case of Ransomwares and Vipers. In order to increase the availability of data, it is recommended to maintain daily or weekly offline backup of critical data in external media like official portable hard disks or DVD drives. Connected backups in cloud storages have limited usefulness for recovery as attackers damage them along with data on devices.

Mitigation Principles

Once an endpoint is compromised, mitigation may seem like a futile exercise but it is not so. Depending upon how quickly the compromise is detected, mitigation will be able to salvage some of the data and prevent further damage. The following principles can help end users minimize loss and recover quickly,

- **Stop Use:** As soon as users become aware of a compromise or suspect a compromise of device, it is strongly recommended to stop use of the compromised / suspected device for all operations immediately till remediation is complete. This will ensure that the damage is contained till that point of time.
- **Disconnect:** Next step is to immediately physically disconnect all network connections to the compromised device(s) to stop the infection to spreading to other devices.
- **Change Passwords:** In order to limit access to compromise accounts for attackers, immediately change passwords of all accounts used on the infected devices from a known safe and clean device. It will ensure that the compromised accounts will no longer be misused by the attackers.
- **System Scan:** Once damage control of existing accounts is done, run a full system scan using the updated antivirus installed on the device. Preserve the device and all files on it for forensics to find the medium and impact of compromise. Unless the reasons for compromise are known, the device cannot be deemed fully secure.
- **Remediation:** Contact the experts to do a full forensic analysis of the suspected / compromised device to find out vulnerabilities used and the impact of the compromise. Also, demand recommendations to protect the device in future from such compromises. Users have to keep in mind that sometimes the compromises will happen even after following all best practices but it is not a reason to abandon them as it will increase the risk of compromise manifold.
- **Format Endpoint:** Once the experts have cleared the device after forensic examination, copy only extremely critical data from the compromised device to external storage and format it completely i.e. all partitions. Only complete format of the compromised device can ensure that the device is clean and ready to use. Install endpoint security agent as the first thing and update the operating system before installing any other software.
- **Restore Data:** Once the system is rebuilt and updated with latest patches for operating system and all other software, copy data from the external backup and the device is ready to use. Every compromise should remind the users of the risks of cyber space and motivate them to follow the basis cyber security hygiene with more rigor and conviction

Summary

This article tries to highlight the importance of endpoints as a new frontier in the cyber warfare, the importance of keeping the endpoint devices safe and make the users realize the significance of their cyber habits and hygiene as a crucial component in the full-blown cyber war. This article also tries to provide a set of best practices that users can follow without the use of fancy technology to prevent compromises to a large extent. It then tries to define some basic steps to follow in case of suspected compromise or actual compromise. The key takeaway is that prevention is better than cure and basic hygiene can save users from a great of pain and ignominy while navigating through the hostile cyber space.

Contact for more details

Syed Hasan Mahmood
Scientist-C
National Informatics Centre, A-Block, CGO Complex
Lodhi Road, New Delhi - 110 003
Email: hasan@nic.in , Phone: 011-24305379