Atense Inc.
CYBER DEFENSE
The Home of Anti-Malware DNA™

ATENSE COMPUTER VACCINE IDEA

SOFTWARE INSTALLED in the Atense's computer vaccine™ platform will be certified that the software is safe and is free from malware.

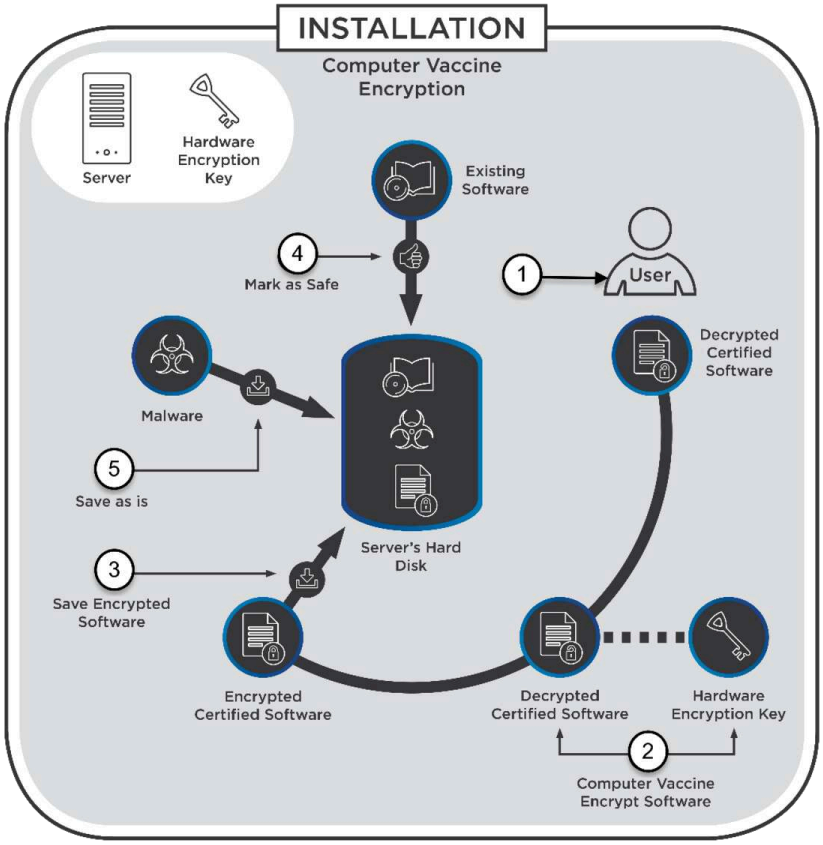
THERE ARE TWO KIND of software certifications: Atense's certified and Enterprise's certified.

ATENSE'S CERTIFIED SOFTWARE will be allowed to be installed in any computing device hosting Atense's computer vaccine™ platform.

ENTERPRISE CERTIFIED SOFTWARE will only be allowed to be installed on computing devices hosting Atense's computer vaccine™ platform belonging to the enterprise which certified the software.

INSTALLATION PROCESS:

(1) User installs decrypted certified software.
(2) The Atense's computer vaccine™ platform using an encryption/decryption key, encrypts the certified software deriving an encrypted version of the software.
(3) The encrypted version in the software is installed computer's hard disk.
(4) Installed software which are present in computer before the hosting of the Atense's computer vaccine™ platform are marked as 'Safe'.
(5) Malware are installed in the computer in its original form without any encryption or being marking as safe.



THE EXECUTION of software follows one of three paths: encrypted certified software, software marked as safe, and malware.

CERTIFIED SOFTWARE, once initiated, is retrieved, decrypted and the clean code is passed to the Operating System for execution.

SAFE SOFTWARE, once initiated, is retrieved as is and passed to the Operating System for execution.

MALWARE, once initiated, is retrieved as is and decrypted. And since decryption is a form of encryption. The malware becomes encrypted and the encrypted version is passed to the Operating System for execution. But once the encrypted malware execution is initiated, it is disabled – and the user is notified with an error message.

EXECUTION PROCESS

CERTIFIED SOFTWARE

(1) A user initiates the execution of a certified software

(2) Using the encryption/decryption key, decrypt the encrypted software

(3) A decrypted software is derived and executed in the computer

SAFE SOFTWARE

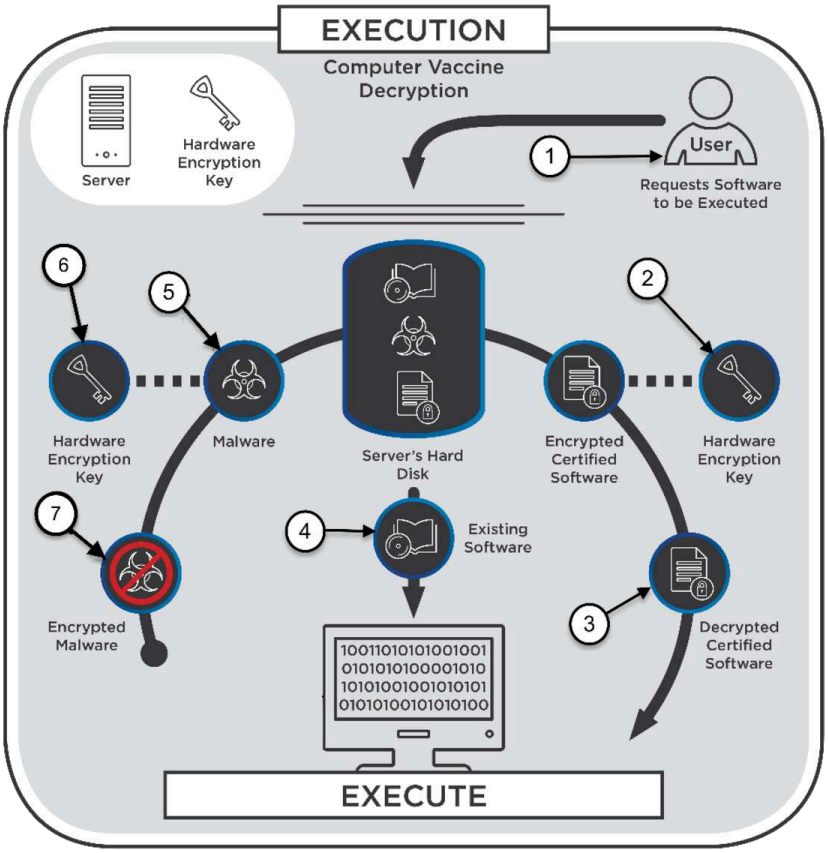
(4) A software which was in the computer prior the hosting of Atense's computer vaccine™ platform and marked as safe is executed in the computer as is

MALWARE

(5) A malware is retrieved as is

(6) Decrypted with the encryption/decryption key. And since decryption is another form of encryption. The malware becomes encrypted

(7) And disabled



A computer hosting **Atense's Computer Vaccine Platform™** offers an unprecedented protection to the computer, where certified and authorized software executes without hindrance – *but malware of any kind is disabled.*

ATENSE'S COMPUTER VACCINE PLATFORM™

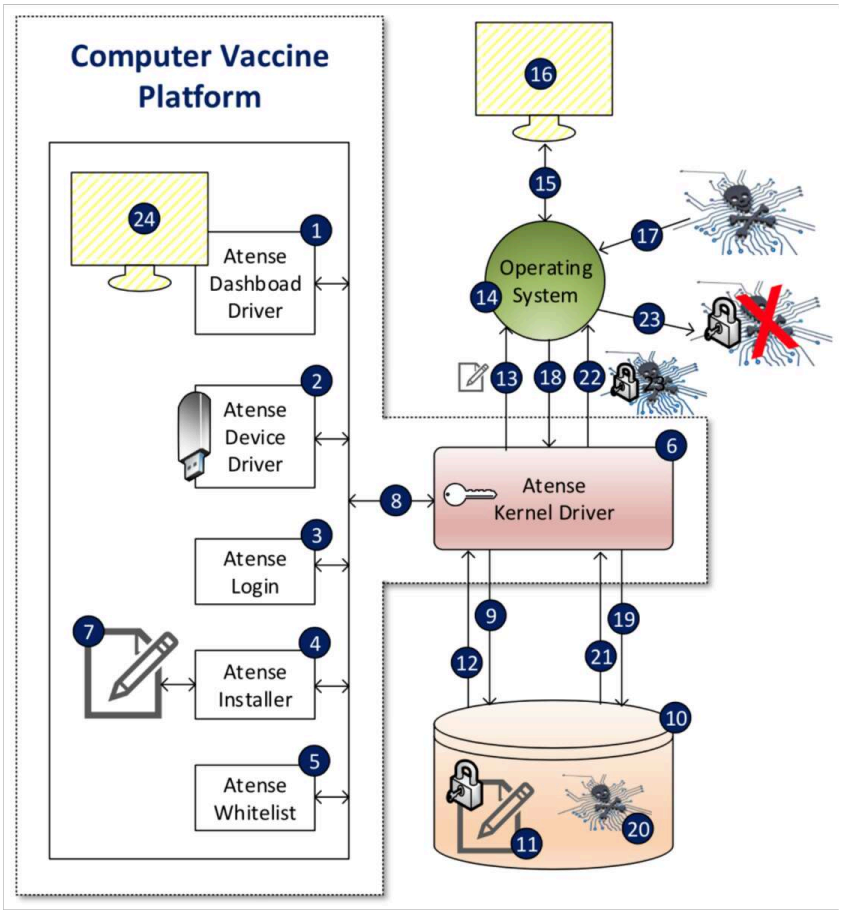
At the startup of the computer hosting Atense Computer Vaccine Platform, the Atense Device Driver (2) reads an encryption key from the USB device and passes it (8) to the Atense Kernel Driver (6).

INSTALLING CERTIFIED SOFTWARE

Atense only installs certified software (7). The certified software (7) is malware free.

A system administrator logs in (3) and the system administrator credentials is transferred (8) to the Atense Kernel Driver (6).

Atense Installer (4) installs the certified software (7) and as the certified software (7) is installed, Atense Kernel Driver (6) using the encryption/decryption key encrypts the certified software deriving an encrypted version. Then saving (9) the encrypted version (11) in the computer's hard disk (10).



RUNNING CERTIFIED SOFTWARE

As the operating system (14) requests the encrypted software (11), Atense Kernel Driver (6) loads (12) the encrypted software (11). And using the encryption/decryption key, the Atense Kernel Driver (6) decrypts the encrypted software (11) deriving clean software code, which is then passed (13) to Operating System (14) and the software code is executed and displayed on the computer's monitor (15)(16).

INSTALLING MALWARE

Once a malware (17) is installed in a computer running Atense Computer Vaccine Platform™. The Operating System (14) passes (18) the malware (17) to the Atense Kernel Driver (6) and the malware (17) is stored (19) in the hard disk (10) as malware (20).

RUNNING MALWARE

When the Operating System (14) requests (18) the malware (20) for execution, Atense Kernel Driver (6) retrieves (21) the malware (20) from the hard disk (10). Then using the encryption/decryption key, decrypts the malware (20). And since decryption is also a form of encryption, the malware (20) becomes encrypted. Then, Atense Kernel Driver (6) returns (22) the encrypted malware to the Operating System (14) and the encrypted malware gets disabled (23). And an error message is sent

(15) and displayed on the computer's screen (16). Also, Atense Kernel Driver (6) send an error message to Atense Dashboard (1) which is displayed on the screen (24).

ATENSE WHITELIST

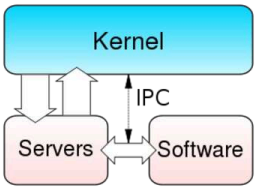
Atense Kernel Driver (6) uses Atense Whitelist (5) to further enhance the security of the computer hosting Atense Computer Vaccine Platform™.

Atense Inc.
CYBER DEFENSE
The Home of Anti-Malware DNA™

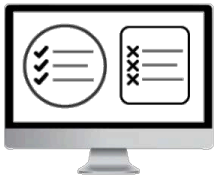
ATENSE COMPUTER VACCINE PLATFORM

We developed a software platform which works in synchrony with the Window's operating system and it controls which software can be installed and also, which software that can and cannot be initiated in the Windows operating system. We named our software platform as 'Computer Vaccine' and filed a trademark protection.

Software certification allows Atense and enterprises to certify software. Atense's certified software can be installed in any computer hosting Atense Computer Vaccine. The enterprise's certified software can only be installed in the enterprise's computers hosting Atense Computer Vaccine.
A certified software will only be allowed to be installed in a computer hosting Atense Computer Vaccine if an authorized user is logged in through our proprietary login software module. Once a certified software is installed, it gets converted into a digital DNA which is unique to the computer.



A kernel software driver is in the core of the Window's operating system and it will only allow software to run in the computer if the software is authorized, or having the computer's digital DNA, or if the software conforms to the whitelisting rules.



Whitelisting programs like Windows' power shell and others is only allowed to run in the computer if an authorized user is logged in through our proprietary login software module. Hackers use Windows programs as entry point to infect and hack a computer.

Computer folder whitelisting based on file type enables only specific file type to be saved in the whitelisted folder. If a website has a flaw and a hacker is able to save an executable file in an image file designate folder, then the hacker takes over the website. But if the folder is whitelisted the attack is prevented because only image file is allowed to be saved in the whitelisted folder.

Computer folder whitelisting based on specific date and time-frame allows files to be saved on a whitelisted folder if it is between the specified date and time-frame. If a website has a flaw, hackers take advantage of the flaw to save executable file in a website folder, then executing it and taking over the website.

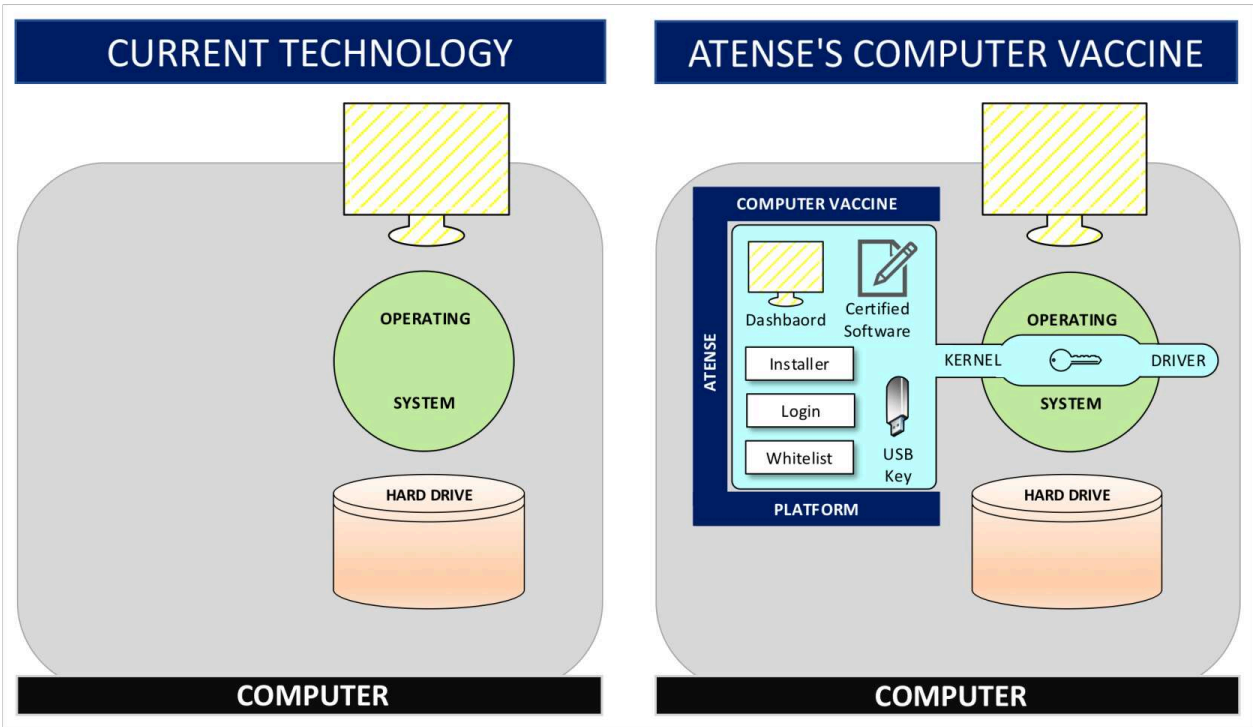
But if the folder is whitelisted with a date and time-frame, this attack is not allowed because the date and time the hacker is attacking the website is not within the date and time-frame of the whitelisted folder. The date and time-frame are only used for the purpose of updating the website and will only be valid at the updating time. Thus, any attempt to save executable file in a whitelisted folder which is outside the date and time-frame assigned to the folder, will be denied.

Critical documents are whitelisted and automatically encrypted and decrypted. And if a malicious insider copies the document or if the document is stolen, the document will still be encrypted and protected. The only way to copy a whitelisted document in a decrypted form, is with an authorized user (system administrator) being logged in through Atense Computer Vaccine.

A dashboard pinpoints the location of a halted hacking attempt and any login attempt through the Atense Computer Vaccine login module. Such mechanism allows the cybersecurity personnel to take immediate response in case of a computer infection, hacking attempt or any legit and non-legit login attempt.

CURRENT TECHNOLOGY VS ATENSE COMPUTER VACCINE

Atense Computer Vaccine differs greatly from current technology as illustrated in the image below.



The current technology has a single way to install and execute program in a computer. For this reason, as long as the operating system is concerned, all software is treated alike. And it includes unintended software, like malware and intended software, like a spread sheet.

Atense Computer Vaccine adds another layer over the operating and it includes its own software certification, installer, login, white listing and a kernel software driver working inside the operating system.

By adding an additional layer, the programs that are installed through Atense Computer platform are treated different than software which are saved in the computer outside the Computer Vaccine platform.

Each computer hosting Atense Computer Vaccine platform has a key which is unique to the computer.

A software to be installed it is certified to be virus free, malware free and ransomware free.

In terms to install a certified software an authorized user, usually a system administrator, must be logged in thought our proprietary login. Once the software is being installed it gets converted to the digital DNA which is unique to the computer.

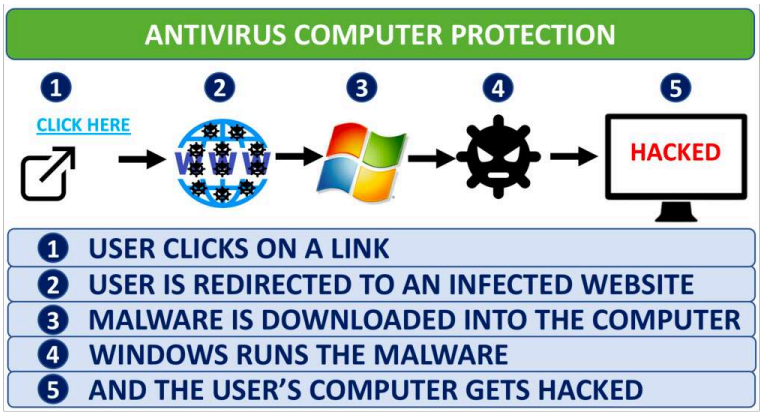
And any software lacking the computer's digital DNA gets blocks. Thus, blocking computer virus, malware and ransomware.

COMPUTER HACKING AND PREVENTION

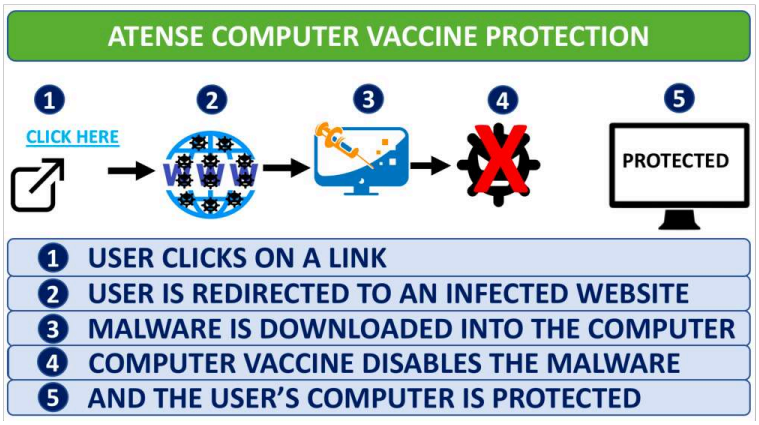
There are many ways a malware can infect a computer. Here are some of the most used methods and how Atense Computer Vaccine stops the same hacking attempt.

CLICKING ON LINK

Hacking: the user receives an e-mail with a link or just click on a webpage's link and the user's web browser is redirected to the hacker's website and if a flaw is present the user's computer or the web browser, a malware is downloaded and executed in the user's computer and the hacker takes over the user's computer.

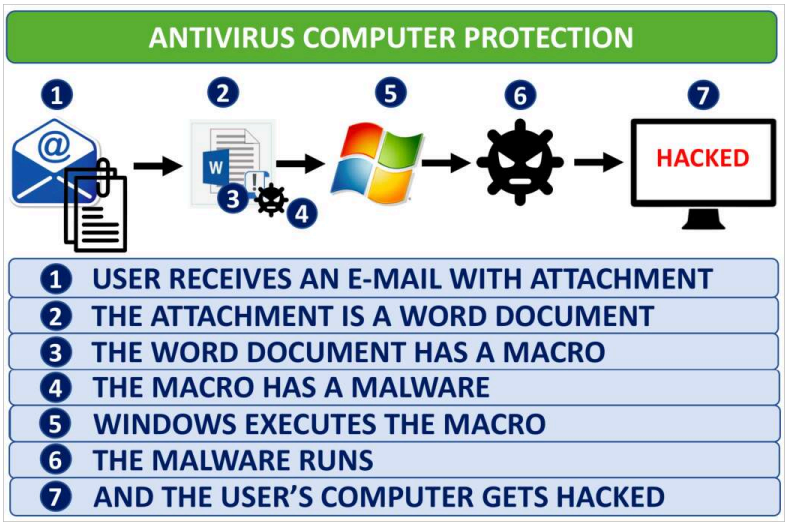


Computer Vaccine Prevention: if the computer or the web browser happens to have a flaw and a malware is loaded into the user's computer. Since the malware is not a certified software, the malware gets disabled and a message sent to the dashboard for proper action.

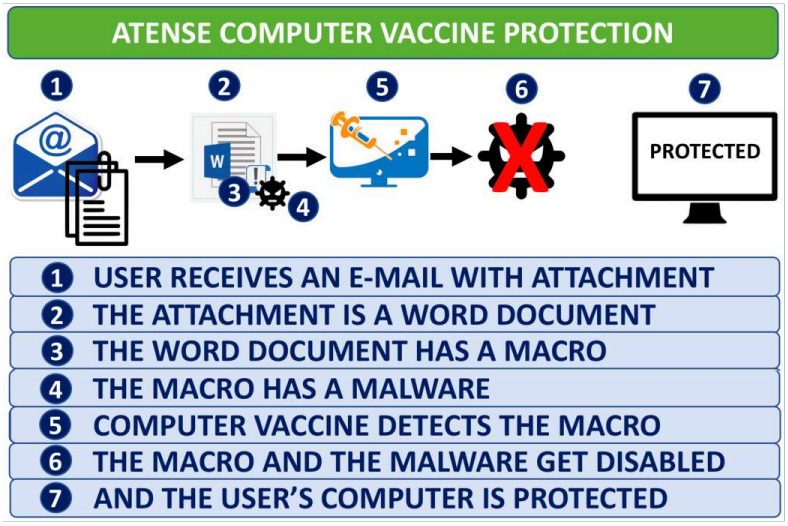


Atense Inc.
CYBER DEFENSE
The Home of Anti-Malware DNA™

E-MAIL ATTACHMENT



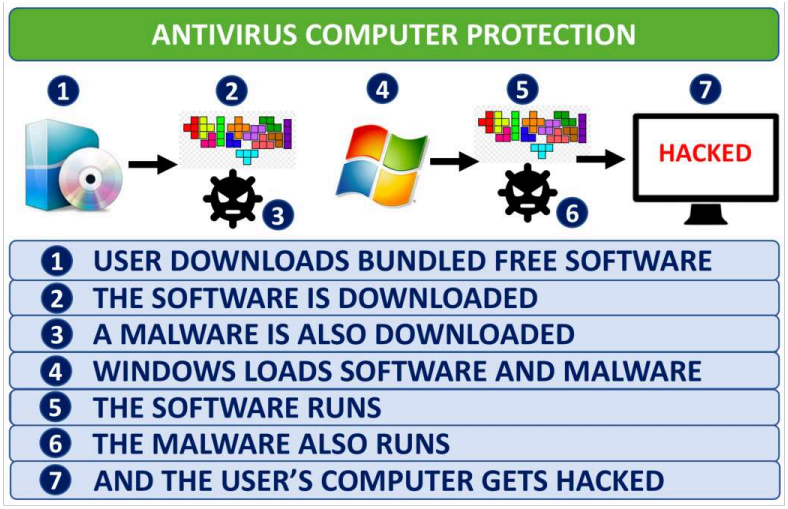
Hacking: the user receives an enticing or urgent e-mail and the e-mail has an attachment with a Microsoft office document, like a word document. Microsoft office documents can have a program called, macro. Once the user opens the e-mail, the e-mail has an enticing or urgent message to trick the user to click on a button to allow the document's macro to execute in the computer. And once the user clicks on the button, the macro executes and launches Windows programs like, power shell. Once the power shell is executed, it opens the computer and downloads malware, then the hacker takes over the user's computer.



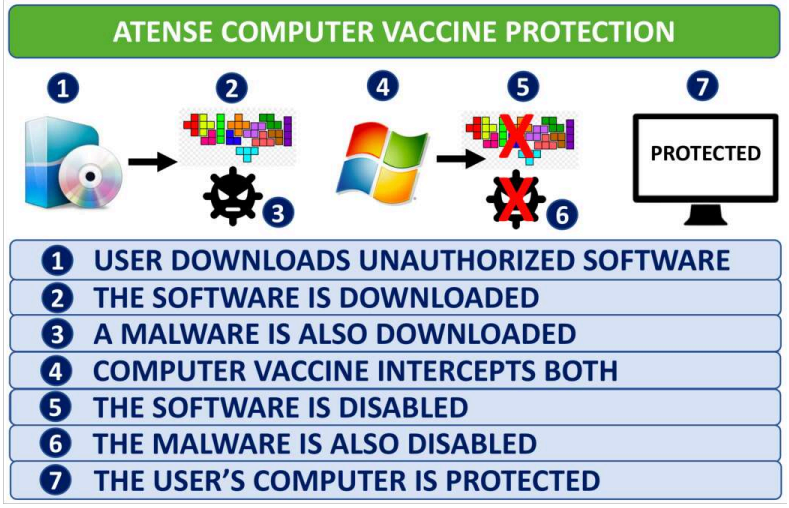
Computer Vaccine Prevention: once the user opens a received e-mail attachment and allows a macro to run, the macro will try to initiate the execution of a Windows program, like power shell. But the power shell program is whitelisted and a whitelisted program is only allowed to run in the computer if an authorized user is logged in through Atense Computer Vaccine login module. Since an authorized user is not logged in, the power shell execution is halted, the macro is disabled, a message is sent to the dashboard and the hacking attempt is halted.

BUNDLED SOFTWARE

Hacking: the user downloads a free software like, a video game. But the free software has other programs which are malware and once the free software is installed, the malware also gets installed. And once the malware runs in the computer, the hacker takes over the user's computer.

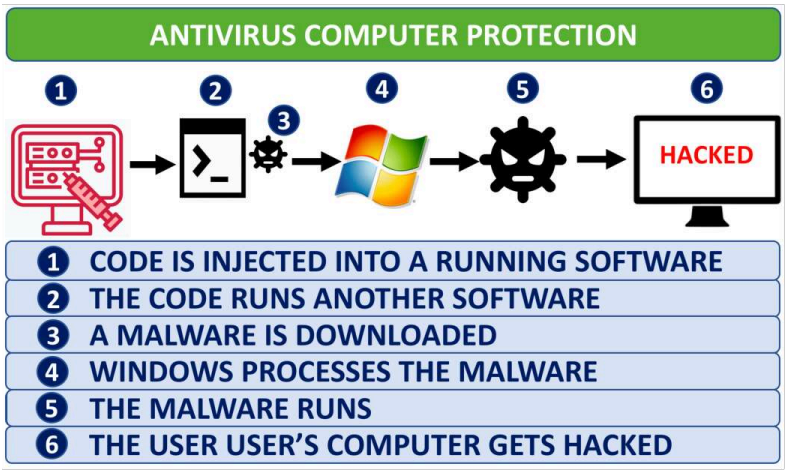


Computer Vaccine Prevention: once the user downloads a software which is not certified, the software and the malware gets marked as virus, gets disabled and a message sent to the dashboard. Thus, avoiding the computer's infection.

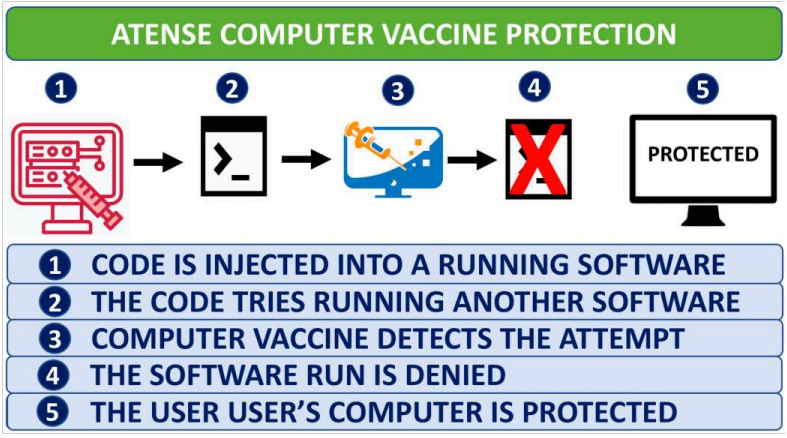


CODE INJECTION

Hacking: a program in computer has flaws which allows code to be injected into the running program. Once the code is injected, the injected code will change the execution flow of the running program and execute other programs in the Windows operating system, like power shell or the hacker gets superuser access to the computer. One way or the other, the hacker takes over the user's computer.



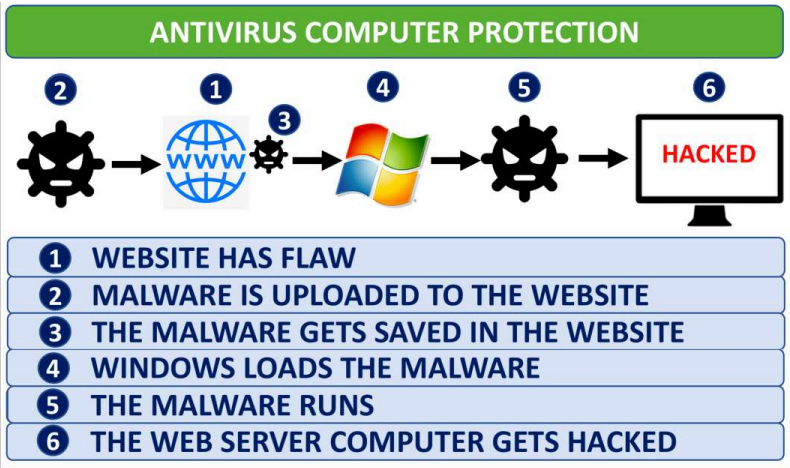
Computer Vaccine Prevention: if code injection attack happens because of flaws in a program running in the computer. Once the injected code or the hacker tries to execute a program like a power shell. Since the power shell is whitelisted and an authorized user is not logged in through the Atense Computer Vaccine login module. The power shell's execution is denied, a message sent to the dashboard and the hacking attempt is halted.



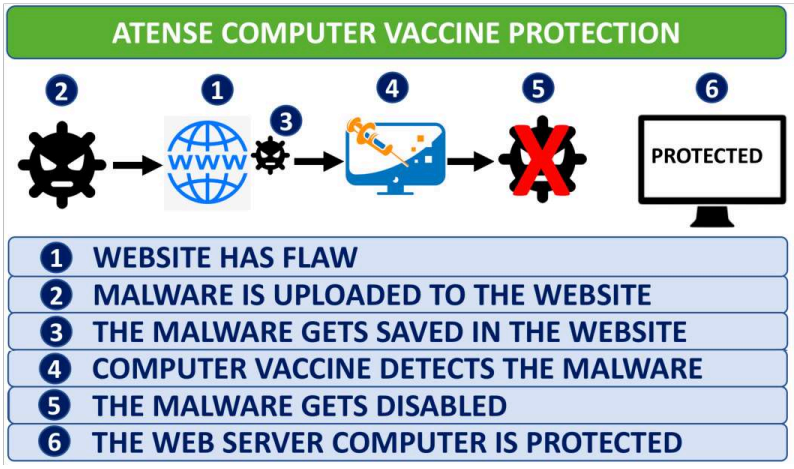
Atense Inc.
CYBER DEFENSE
The Home of Anti-Malware DNA™

WEBSITE VULNERABILITIES

Hacking: if the website has a flaw, a hacker is able to send an executable file to the website and then execute the file's code and take over the website.

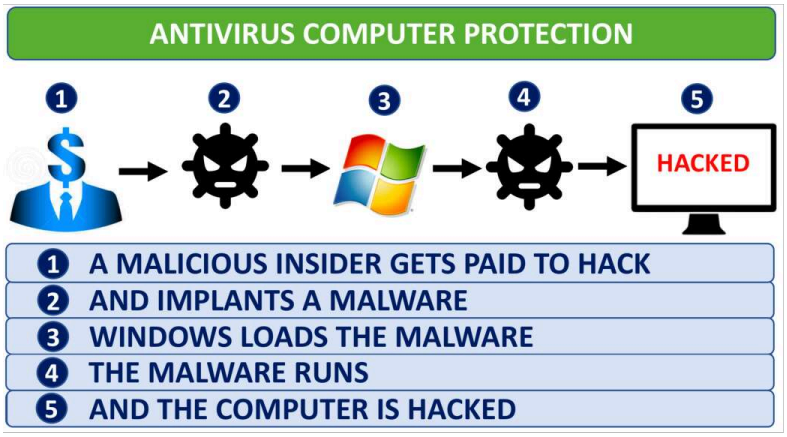


Computer Vaccine Prevention: if a website happens to have a flaw and a hacker is able to send an executable file to the website. Since the website folder is whitelisted. And the whitelisted folder only allows the saving of specific file type at the specified whitelisted folder. Or, a file is only allowed to be saved in a whitelisted folder at specific date and time-frame. Since neither of the parameters are valid, the attempt is halted, a message is sent to the dashboard.

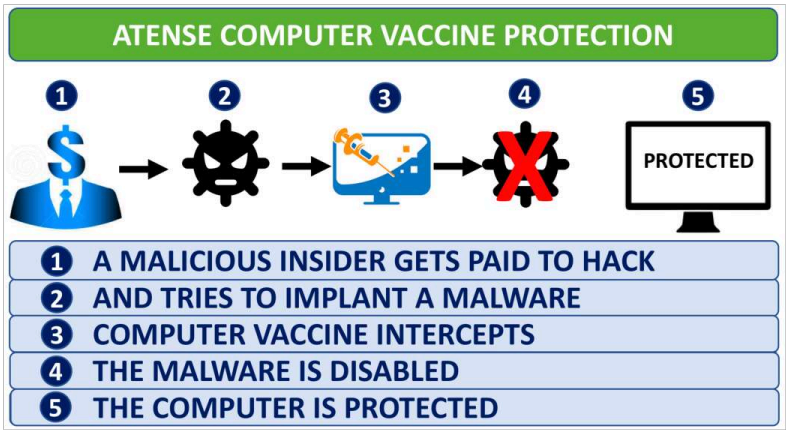


MALICIOUS INSIDER HACK

Malicious Insider: Malicious insider is motivated to harm the organization and can be an employee, a vendor or a hacker. A malicious insider is harder to stop because the individual is already inside the organization and in many cases, having knowledge of the organization's network.

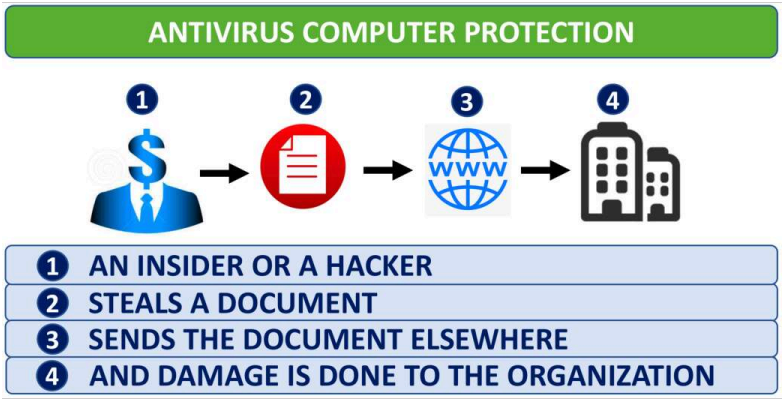


Computer Vaccine Prevention: Once a malicious insider tries to install a malware in the organization's computer, Atense Computer Vaccine detects and disables the malware. The attempt is halted, a message is sent to the dashboard. Even if the malicious insider is a network administrator, still will be stopped because the dashboard will display the Atense Computer Vaccine login attempt and a non-certified malware cannot be installed.



MALICIOUS INSIDER STEALER

Malicious Insider: The malicious insider steals a file and the file has confidential information. Then the file is given to others. The reason varies, but the end result is to harm the organization.



Computer Vaccine Prevention: Atense Computer Vaccine encrypts whitelisted files and the encryption and decryption of the file is done automatically without user intervention. If an encrypted file with confidential information happens to be stolen, the file still encrypted and is useless.