Kailax technical details

Buro Jansen has previously written about Kailax in the article 'Kailax / Nir (Max) Levy; The magic hand of Israeli intelligence'. This piece focuses on some of the technical details of the Unlocker and a few mysteries that still need solving. All of this information is coming from the HackingTeam leak that happened in 2014.

Unlocking locked Windows computers

Kailax has two solutions at their disposal. The Unlocker and the add-on U-Cap. Let's focus on the Unlocker tool first.

Kailax's Unlocker is a hardware device that can be attached with a USB to the victim's Windows computer to bypass the Windows lock screen.

Envision that you leave the house to visit friends, you shut down your computer and imagine that no one can mess with it. They simply don't have the password. Most IT-security people think different about it and the surveillance industrial complex has a lot of solutions to get around some of the security features that you might have enabled.

A malicious actor doesn't need your password in order to unlock the computer and plant spyware or worse, get control of an administrator account.

The same applies when the computer is powered off. It seems that full disk encryption is a possible solution to prevent unwanted entry into your computer.

However, most solutions present only partial disk encryption. This is due to having 2 separate locations on your hard drive, a boot partition and the encrypted data partition. The boot partition is an unencrypted partition and therefor vulnerable to tampering.

Most commercial operating systems and software running on them, do not have an option available to mitigate the partial encryption problem.

However, if you would run a free and/or open source system, you can achieve full disk encryption.

The Unlocker works on all x86 and x64 versions of the following operating systems:

* Windows Vista

* Windows 7

* Windows 8

* Windows 8.1

* Windows Server 2008

* Windows Server 2008 R2

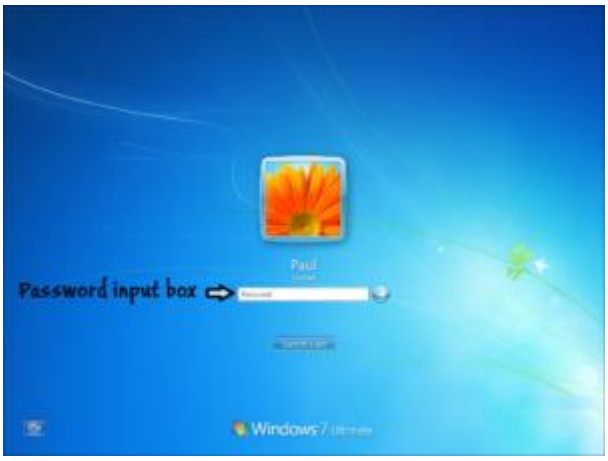
* Windows Server 2012

Server Core (no GUI) versions of Windows Server are not supported.

Note:

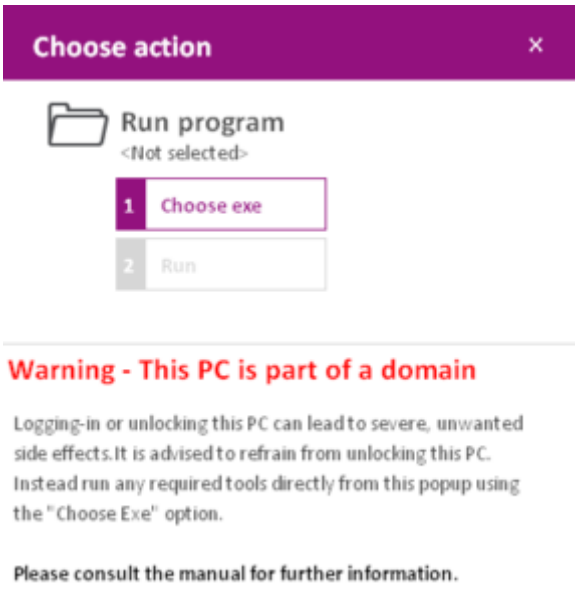
As you can see, Windows 10 support is missing from this list. At the time of the leak, Windows 10 hadn't been released. At the time of writing we're unsure if Windows 10 is supported by either the Unlocker or U-cap.

After the Unlocker is attached to the victim's computer, a new screen appears in purple, it will ask you to either launch an executable or bypass the lockscreen.



If you alt-tab you will see that the purple screen disappears and allows you to click on the password input text box. If you now put in a single letter and click enter, the PC will be unlocked and Windows will switch to the user desktop. The same attack will work for any other users that may exist on the same computer.

As Kailax indicates in their user manual: "You can use the Unlocker to bypass the Windows password and use the PC like a regular user. This option should be used with extreme care if stealth is required, and it is the user's responsibility to put the PC back in the same state as before the unlocking once done. Before bypassing the password, check if there's a warning at the bottom of the purple popup screen stating that the PC is part of a Domain."



However, if absolutely necessary, as Kailax indicates, it still might be possible to bypass the password, even if the PC is part of a Domain. An extract of their user's manual follows below:

The recommended and stealthiest method to use the Unlocker is through the "Run program" option. If bypassing the password is absolutely necessary, read the following carefully:

* Bypassing passwords on PCs that are part of a domain will only work if Cached Credentials are enabled in the Group Policy of the Domain Controller.

* Bypassing passwords on PCs that are part of a domain will cause a brief network disconnection. As a result, any existing VPN connections will likely disconnect.

* Trying to bypass the password on a domain PC when it is locked (as opposed to when a user has yet to log-on) will work, but will set the user's cached password to the password entered during the bypass. It will therefore be impossible to log-on or unlock the PC in the future with the *correct* password if the Domain Controller is unavailable. This password re-set will last until the correct password is used to unlock or logon AND the Domain Controller is available through either LAN/WAN or a VPN.

This means that in most real-world scenarios, bypassing the password on a PC that is part of a domain AND is connected to the domain through a VPN will lock the legitimate user out of their PC until they connect to the organization’s LAN/WAN.

* Trying to bypass the password on a domain PC with a user that is not currently logged on may work, but is likely to cause the PC account to be locked on the domain, so that only the Domain Administrator can release the account and make the PC usable again.

* Some typical enterprise client side software, for example Outlook, SharePoint client, Lync and others may behave unexpectedly, and in particular require re-authentication.

The Unlocker comes with an mute device that can be inserted in the audio out jack. This is to make the attack be silent, since when an USB device is (dis)connected it makes a sound. Or mute it when the keyboard allows you to.

In addition, Kailax' Unlocker comes with an included a USB flash drive. You can use the drive to store forensics software and other tools you may wish to use on target PCs, and/or save downloaded data onto it.

It should also be noted that the Unlocker works, even if the Autorun option is disabled in Windows.

U-Cap

U-Cap is an add-on for the Unlocker tool that enables the use of a so-called payload to deliver spyware to the victim’s computer or execute a payload with SYSTEM privileges, which is the equivalent of having full administrator control on the computer. A working Unlocker with version 1.3 is required to be able to use the U-cap device.

From the U-Cap user manual:

Step A

- Check the state of the target PC:

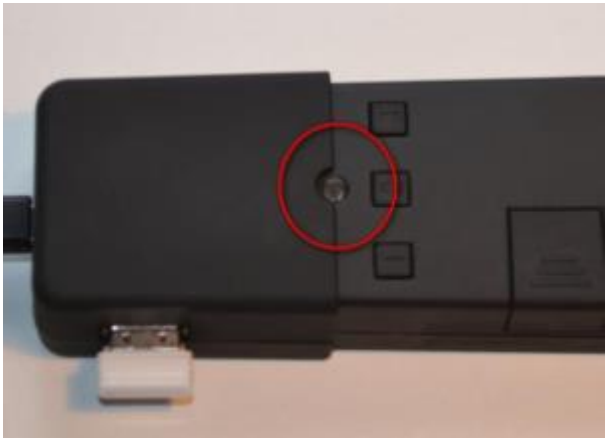
* If the PC is powered off - start the PC (power on), and wait for the logon screen to appear. Once the logon screen appears, wait an additional two minutes for background services to complete loading, then continue to Step B.

* If the PC is powered on but not locked, you can use the U-Cap to execute your payload with SYSTEM privileges. To do so, start by locking the PC (via the windows menu or by hitting windows key + L) and then continue to Step B. **Note** however that after a successful execution the PC will remain locked.

* If the PC is locked - continue to step B.

Step B

Connect the U-Cap unit to the Unlocker unit until semicircular indentation on U-Cap engulfs the LED indicator on the Unlocker unit.



Step C

Plug in the pre-formatted and payload loaded Flash drive into unit USB plug

Step D

Plug in the Micro USB connector of the Unlocker USB cable to U-Cap's Micro USB socket.

Step E

Plug in the other side of the USB cable into any free USB port on the target PC. If possible, use a USB2 port and not USB3 (blue) port.

Step F

Follow the steps as detailed in the table below – these are the same steps as running Unlocker, except for the last stage.

How do they do it?

Unfortunately, how they manage to pull off those attacks are not clear at the time of writing. Kailax is very protective of their intellectual property and no details can be found in the documents

that are leaked or through the discussions they had via e-mail. We're not sure if this is because of a so-called Zero Day or a Windows feature they're abusing.

Please refer to the Kailax FAQ.pdf for additional minor technical details.

To be complete it should be noted that there are off-the-shelf commercial devices like FinFireWire

(https://wikileaks.org/spyfiles4/documents/Release-Notes-FinFireWire-3.5.=pdf)

and open source frameworks like Inception that can target operating systems like MacOS, Windows and Linux using 'direct memory access' or short DMA. Some examples of those ports are Thunderbolt, Firewire, PCI(e), Cardbus or Expresscard. DMA allows data transfer at a very high rate between devices like camera's or storage devices, but it could also be exploited by an attacker to retrieve parts of the memory of a running computer where sensitive information might be stored.

Many experts agree however that, if you leave your computer unguarded and an attacker has a window of opportunity, the device should be considered compromised.

If you have any information or samples to share, please e-mail the author: drwhax [@] riseup [dot] net

Jurre van Bergen

Kailax technical details (pdf)

Gehele Observant #71 Niet Transparante Overheid en Wetenschap (pdf)

Kailax / Nir (Max) Levy; The magic hand of Israeli intelligence

Kailax / Nir (Max) Levy; The magic hand of Israeli intelligence (pdf)

Providence and the Dutch National Police Supply chain liability via a former police officer (English translation of article from Observant #69)

Security Industry: links between Israel and the Netherlands? an inventory

Wikileaks Hacking Team documenten

Enkele e-mails uit HackingTeam gegevens over 2beuropa

Enkele e-mails uit Hacking Team over Kailax

Statement of Work Hacking Team en Kailax