BIZCOMMUNITY

Why you need to be very, very aware of LoJax

By Bryan Hamman

5 Apr 2019

The conventional wisdom with malware is that you can kill it once and for all by wiping a system and starting from scratch. However, a particularly clever piece of surveillance software with Russian ties appears much more resistant. Even replacing drives won't kill LoJax, which is still active more than nine months after researchers from Arbor Networks detailed it.

A report on Extreme Tech warns that ‘the only way to purge the malware is to wipe the hard drive and flash the motherboard firmware (although, it’s probably safer to just throw the hardware out).’ This specific piece of malware is insane

Bryan Hamman, territory manager for sub-Saharan Africa at Netscout Arbor

LoJax was built by Fancy Bear, a Russian cyber espionage group who specialise in Advanced Persistent Threat (APT) cyber-attacks, and is a Unified Extensible Firmware Interface (UEFI) based rootkit that behaves as a double-agent, leveraging legitimate software to phone home to malicious command and control (C2) servers.

Most frightening is that, although we think it was created in 2016, it has been active for over nine months and is still causing havoc by using UEFI and pre-installed Computrace LoJack software to locate and lock devices remotely, deleting files and similar, making it an effective laptop theft recovery and data wiping platform.

It is proving resilient to hard drive replacement and Windows OS re-installs and, as mentioned in the above article, businesses are faced with no option but to destroy hardware in an effort to remove it from their systems.

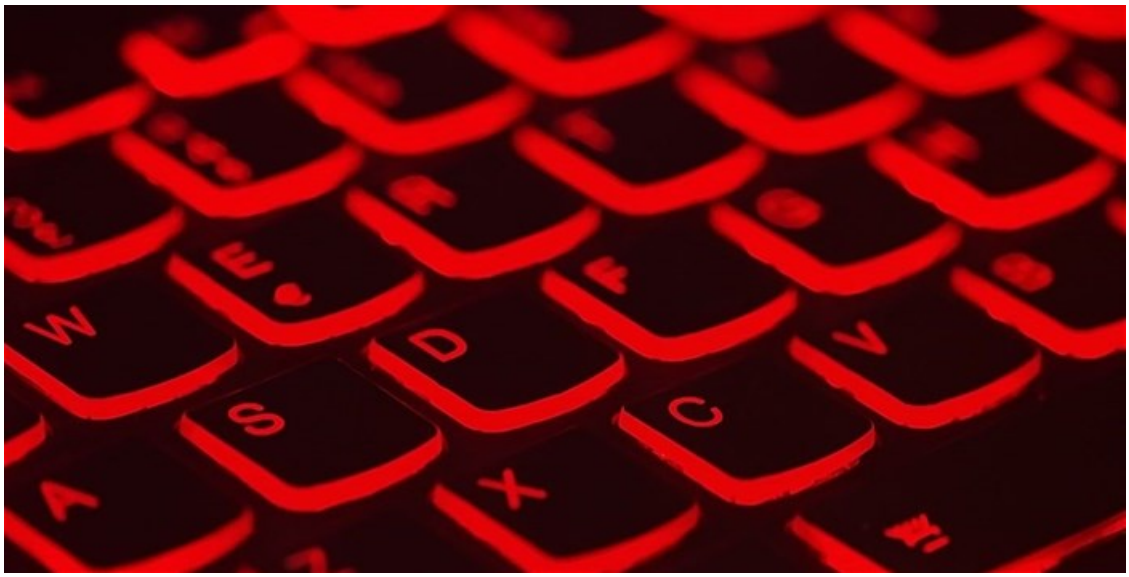
The challenge in defeating LoJax lies in the fact that UEFI and Computrace LoJack are considered safe and necessary components and most corporate cybersecurity solutions have been created and built with this understanding.

Prevention is the key

The general understanding around how LoJax infects systems is most often, though not always, through every day spear phishing.Spear phishing is an email attack that targets a specific organisation or individual, seeking unauthorised access to sensitive information that will ultimately result in the delivery of financial gain, trade secrets or military information.

These emails appear to come from a trusted source and can even seem to be sent by well-known organisations like Virgin or FNB. So, while very dramatic steps will need to be taken once LoJax has infected your systems, there are less destructive steps that can be taken to stop the initial infection.

Because this type of malware generally requires a manual or case-by-case installation and is not something we've observed propagating automatically, these steps rely very much on user education and user adoption of company security protocols.



Quickly evaluating bad hygiene or potential threats in an email may seem simple to those in the know but it is often not the case with everyday people.

A good place to start is by circulating a cheat sheet on what to look for before you click that link and an article written by Ifeanyi Egede that did the rounds last year sums it up quite nicely:

1. **Check the sender email address**: most of the time when an email that seems odd coming in from what looks like a trusted source, links are simply clicked. A new procedure might include making sure email addresses are checked before any other steps are taken. They may be able to spoof the email address to a point but, generally, one or the

other will be suspiciously different to normal emails received from the person they are mimicking.

2. **Check the email format**: advanced spear phishing email attacks may be able to spoof both the email address and sender's name and, in these cases, the format of the mail might hint at the legitimacy of the content shared. The signature or the format/font/spacing of the email may not match the usual format used in previous communications. If something looks wrong, take extra precautions.

3. **Pick up the phone**: if the email you're reading looks or feels wrong (consider typos, *CAPITALISATION* or even simple spelling errors in an email from FNB, for example, where most content is automated), it's probably wrong. Pick up the phone and call the sender to double check whether it is indeed them sending the correspondence.

4. **Verify before you click**: Some attacks will ask you to click on a link for further information. Hovering your mouse over this link will guide you – an email from Virgin should contain links that lead out to its web site properties, not anywhere else. One click can lead to malware like LoJax infiltrating and taking control of your system – rather err on the side of caution. Having said that, if links are clicked and you are asked for a password, pin or account number, immediately close the page and contact IT.

5. **Scan the attachments**: When attackers manage to bypass all of the tell-tale signs and trick users into downloading email attachments – a good standard procedure to implement is scanning of attachments for embedded viruses or code prior to opening. This is a solid rule to enforce regardless as to how suspicious the email sender may be as any files attached to an email can be dodgy.

When we consider how many malware threats can be avoided by simple user education, it's easy to see the type of procedures that need to be introduced.

Where LoJax is concerned, for now, we'll continue to scan and monitor its progress, updating our product sets as and when more intelligence surfaces. On our blog, we've shared a Yara signature to help identify the agent. Additionally, IT administrators can look for C2 communications coming from the software and verify if it is legitimate or a known bad C2. If there is LoJax on the system, flashing the firmware or replacing the firmware will remove the threat.

ABOUT BRYAN HAMMAN

Bryan Hamman is a territory manager for sub-Saharan Africa at Arbor Networks.
- Why you need to be very, very aware of LoJax - 5 Apr 2019

View my profile and articles...