

Advanced Persistent Threats

An NLAWRP Whitepaper



 NLAWRP

Advanced Persistent Threats (or APT's) are usually directed at Business or Politically aligned sites. Due to the high levels of awareness, it is infrequent that such attempts are made to penetrate militaristic sites.

Usually, an attack is aligned at data harvesting and are far more elegant than a simple 'financial gain' goal such as financial information from bank accounts etc. Usually the systems that are attacked and compromised continue to operate and be of service after any breach.

The method of attack is normally reliant on more elegant software than is normally found and invariably the programming is bespoke and aimed at a particular target where other targets would not be breached using the same protocol. The objective is usually exploitive but frequently there is a factor attendant that will delay immediacy, an inclusion that tends to mask the attack factor being recognized instantly. The dormancy of the data recovery can, in most cases, be programmed and will be actioned later than the attack taking place.

Persistence describes the concept of the genre. The attacks are initiated to introduce a form of 'siphoning' malware into a processor that may respond to later instruction and will lie in wait to be initiated unless there is a contained instruction that demands a report of data at a given date/time or repeatedly on a diarised basis. The attacks are often conducted on a continuous monitoring basis in order to achieve the defined targets. It does not mean that a barrage of attacks and malware insertions will be evident. While the attacks will seem to have a docility about them, in truth the attack is insidious in that the recovery of data may take place at odd hours or by externally commanded execution not necessarily on a prescribed time based periodicity. The intrusion will lie hidden within the system protocols sometimes labeled as a routine that belies its real purpose of data harvesting. The identification is thus made all the more difficult for a legitimate sweeping and exclusion operation to be successful.

The term 'threat' in this case indicates that there is a level of associated human involvement and that the attacks rather than being mindless and automated pieces of code are aimed at an identified areas of data and are under the command of a human operator.

Unlike the intrusive low level attacks that rarely have any strategic alignment, APT's are targeted at specific systems and users to recover sensitive data and not just to disrupt any computer system that they happen to accidentally find through Internet distribution.

This then sets them apart from the malware created by the amateur hacker who rarely has any agenda in mind other than nuisance value or the erasure of the users vital data.

In the case of an attack from an APT, usually there would be little evidence that such an attack had been made simply because the creation of the intrusive item would be such that its tracks and very existence will be so effectively camouflaged that no residual indication of the intrusion will be found, nor for that matter any direct evidence of the attack result being discoverable.

A key requirement of any APT is stealth coupled with a form of cosmetic that will cause the investigating software to miss the real identity when such a sweep is initiated.

The residency in one computer following a dedicated attack is rare and the agility of such intrusions can place the attacking element in any one of a number of computers each with a commonality to its associates, probably by a network connection or by a physical distribution as a contained intrusion hidden in a legitimate data recovery command structure. In this way the threat is mobile and much harder to isolate and identify and its existence becomes so much harder to locate. It becomes a 'piggy-back' intrusion that is distributed by normally legitimate protocols, a very good way of gaining access and to then lie undisturbed until it is 'woken' by the originator.

In the computer security world, APT is used to specifically refer to a subset of threats in a long term pattern of targeted sophisticated hacking intrusions aimed at the primary targets certainly, but in turn, intended to compromise the data of the principle targets locations and ultimately the owners of the hosting systems.

APT violations of computer sanctity in the West are more often well publicized by private organizations but rarely by national organizations and Government installations. The high profile targets are usually unaware that their security structure has been compromised until such time as the applied results of the attack become known. The strategic power attributable to such attacks can be paramount if used correctly, leading to the erasure of a company by such things as 'insider-dealing', a matter that could wipe a company out financially and equally by it being done in a covert manner that the process could be repeated over again, so creating a form of monopolistic action and not necessarily by competitors but potentially by States wishing to gain political and or economic advantage over other administrations.

As an example, the economics of some of the American Southern States are profoundly reliant on market trading futures such as fruits and meat. One of the most valuable of these is the selling prices of such things as 'Pork Futures'. To gain illegal entry into a strategic computer that would report the actuality of real time prices as well as trends could present a major advantage to any competitor who would consider such data to be invaluable. The acquisition of data on a harvesting basis then becomes so valuable that a potential war could ensue with one set of APT's buried in one computer fighting it out with another set of APT's in another company's computer in order to achieve superiority of data validity and hence a market advantage recovered from 'trend' information and projections.

It is to be expected that any major network user under such circumstances will be fully aware of the threat factor and in advance of the execution taking place, will have installed adequate protection to identify the existence of any APT's and have the capability to neutralize them accordingly.

It is however, not the fault of traditional security tools that they cannot deal with APT's as they are not designed to do so. This is due to the development time factor that has been enjoyed by the new breed of hackers who have learnt a lot from the intervening years of simple intrusive and disruptive virtually insignificant system architecture development, that has gone on to become a seriously advanced science.

It goes without saying that the implications for disruption in national economy's has such importance that constant guarding against APT's is mandatory. The 'bloodless coup' potential is high and could eventually result in the redrawing of maps of administrations.

Bibliography and sources

Carr, Jeffrey (date not known)title "*Is the Advanced Persistent Threat a 'who' or a 'what'?*"

Recovered from Internet 05 March 2011. Publisher not known other than Carr.

(Argues for consideration of APT as a process {"attack-process"} and cites specific identities by name as originators)

Damballa (author and date not known)title "*Advanced Persistent Threats (APT)*"

Recovered from Internet 05 March 2011. Publisher not known other than Damballa.

(Identifies the concept of the term and analyses the individual words attributable to the three letters. Also discusses the methods used to infiltrate APT into systems)

Mandiant(author and date not known)title "*Advanced Persistent Threat*"

Recovered from Internet 05 March 2011.Publisher not known other than Mandiant.

(Identifies concept and indicates targeting towards Defence Industrial Base{DIB}, financial industry manufacturing and research industry. Highlights the difference between dedicated intrusion to target and 'casual' 'drive-by' hacking. Recognises the capacity of target administration to develop improved responses to renewed intrusions by analysis and remedial actions).

Wikipedia (author and date not known)title"*Advanced Persistent Threat*"

Recovered from Internet 05 March 2011 (see note below re. publisher)

(Content abstract is virtually word for word of text submitted above by Damballa. Slight differences noted in sentence construction but essentially the same content without additional information)

Analysis

All reports point to agreement of what APT refers to. "A series of intrusive attacks to specific target computer systems in order to recover sensitive (usually financial) information as an indication of economic status of target. Normally introduced and camouflaged to prevent identification".

Following insertion, lies dormant until activated by the targeting source. Differs considerably from low level virus attacks that are usually intent on disruption not data harvesting.

For more information about the National Local Authority
WARP, please visit www.nlawarp.gov.uk.

Paper prepared by Clive Collins.
March 2011.

The logo for NLAWARP features a grid of 24 circles on the left, arranged in 4 rows and 6 columns. The circles are in shades of green and white. To the right of the grid, the letters 'NLAWARP' are displayed in a bold, sans-serif font. The 'N' and 'L' are light green, while 'A', 'W', 'A', 'R', and 'P' are dark green. The second 'A' is stylized as a triangle with a small green dot inside.