Lights Out in Isfahan

pylos.co/2021/12/30/lights-out-in-isfahan/

Joe 12/30/2021

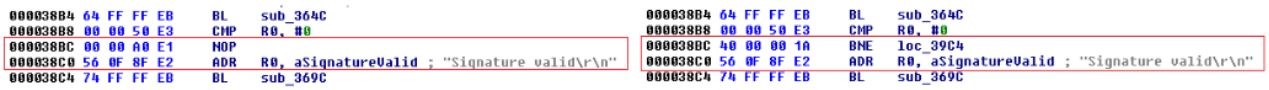

Figure 8 - Disabling the signature validation function in the Bootloader

Iranian security company Amnpardaz Soft published an intriguing report on 28 December 2021 concerning a firmware-level rootkit in HP Integrated Lights Out (iLO) products. While frustratingly containing no Indicators of Compromise (IOCs) – not so much for defensive purposes, but for validating research and independently analyzing artifacts – the report does offer sufficient technical detail to indicate *something* was discovered, and that it appears designed to repeatedly wipe infected systems for a disruptive effect.

The report is interesting for several reasons:

1. The targeted HP iLO technology – while previously rumored to have issues and potential related operations – has no prior confirmed, publicly known capability targeting its use for destructive operations.
2. The capability deployed is designed for a seemingly contradictory combination of stealth, persistence, and potentially destructive purposes.
3. The identifying company, Amnpardaz, is an Iranian entity that appears to only provide software security products to the Iranian market.
4. Details in the report itself emphasize Iran-specific use of the malware in question, at least in terms of identified targets.

Before proceeding further with the iLO malware, a bit of perspective is helpful. For nearly two decades now, Iran has been the subject of a persistent, occasionally spectacular cyber sabotage campaign. Starting at minimum with the Olympic Games program, of which Stuxnet formed a notable part, and proceeding through multiple disruptive operations of varying degrees of sophistication more recently, Iran is no stranger to malicious cyber operations.

Most items over the past three years have been rather overt and relatively simplistic in nature – disruptive events readily identified even if not immediately attributed to the responsible parties. Given past events such as Olympic Games, we can assume that other projects are likely going on at higher levels of sophistication and care. This assumption is supported by more complex, hybrid operations, especially targeting Iran's nuclear program,

involving physical destruction and extrajudicial killing. With continued tensions over Iran's nuclear program as well as other concerns, we should reasonably suppose that interested parties would engage in more clandestine or quiet disruptive campaigns (like Stuxnet itself) in addition to spectacular acts of physical destruction.

That background in mind, that a Tehran-based security company identified a rootkit facilitating system wiping with victimology focusing on Iran becomes quite interesting. The nature of the technology – remote server management software – means its installation footprint will almost certainly extend to a variety of sensitive or high-value systems, from data center management to critical infrastructure applications. While available information cannot determine precisely what iLO instances were targeted, the possibilities for high-impact scenarios are quite strong.

As an aside, you may wonder why an HP server management product would even be an item of interest in Iran, given various sanctions limiting the export of entire categories of technology to the Islamic Republic. However, multiple investigations show various entities engaged in sanctions evasion with respect to HP products specifically for delivery to Iran over the past 20 years. While iLO and related HP servers are not explicitly mentioned in the linked investigations, we can reasonably assume that *some* HP technology made it to Iran, and that these product categories were likely represented in such shipments.

Moving back to the malware, the report from Amnpardaz notes the peculiar functionality of the rootkit in question. While installing to a location both difficult to diagnose and difficult to eradicate (following some modification to firmware verification steps), the malware appears designed for a specific, singular purpose: to wipe the disks of the infected system. But in doing so, this wipe takes place *multiple times* using both a wiping timer, and a countdown timer for the number of wipes to perform.

This repeat functionality is incredibly interesting, as typical wiper malware – from Shamoon to NotPetya – is a "one time only" affair for the impacted system: the malware executes, wipes the host it is located on, and the affair is over. However, given that the iLO rootkit is installed on management application for systems (running separate from the system itself), an interesting capability emerges where a persistent infection can be maintained on a device through the iLO instance to allow for multiple wipes of the same systems on which the malicious firmware is installed. Such capability is not merely disruptive, but incredibly frustrating if not caught as it leads to "ghost in the machine" like worries where operators and IT personnel are unable to determine precisely how or why given systems wipe themselves on a semi-regular basis.

The above is superficially reminiscent of the initial stages of the Stuxnet event. In this case, earlier variants of Stuxnet were designed not to completely destroy the centrifuge hall in Natanz, but rather to induce a loss of system integrity creating pseudo-random failures in the underlying physical system. The goal in this case wasn't to simply destroy the entire enrichment facility, but rather to induce doubt and uncertainty as to the very reliability of the

domestically-produced enrichment technology. Put in simple terms, Stuxnet was a “mindfuck” for the engineers and operators at Natanz, to call into question the technical efficacy of the entire Iranian nuclear program rather than just destroy some (but not all) centrifuges.

The iLO malware echoes this in its subtle, relatively stealthy persistence in an administrative tool in order to disrupt controlled servers. The attacker in question could engage in a persistent campaign of regular system wipes without a risk of likely detection given the described nature of the malicious firmware. Such a situation goes beyond just “we have malware” to a far more insidious circumstance of “do we even understand what is going on with our machines.” This again approaches “ghost in the machine” territory where the very integrity and capability of underlying systems cannot be confirmed or verified, inducing uncertainty and disruption into the entire operation.

In unpacking the iLO malicious firmware in such a fashion, it may thus appear quite obvious who is responsible. Given past analysis of capabilities such as Stuxnet and the overall Olympic Games program, the United States and Israel rapidly come to the forefront as parties with both the technical ability to execute such a campaign as well as the motivation to do so. However, I would strongly caution anyone from making such a quick (and arguably lazy) assumption. While the iLO capability is certainly novel, targeting this application is not completely new (as noted previously) and represents a more common attack development problem than the intricate cyberphysical relationships observed in Stuxnet’s execution. Furthermore, the proliferation of cyber capabilities and offensive tool development mean that any number of state-sponsored entities or even commercial firms may have the know-how and resources to develop a tool such as that observed in this campaign. We ultimately cannot, based on limited available evidence, make any real assessment of “who is responsible” at this time. The US or Israel may represent logical choices, but I would strongly caution curious parties to not write off spunky intelligence organizations with demonstrated sophistication in cyber operations (AIVD and DGSE come to mind) or entities such as various Gulf monarchies simply procuring these types of capabilities for their use in retaliation for Iranian disruptive events in these areas.

In addition to the above caution on attribution of this event, we should also exercise some caution with respect to the very existence of the incident itself. The reporting party, Amnpardaz, is hardly a known quantity in research circles. There is also some potential motivation by Iranian authorities to cast potential disruptive events as part of an external plot, both to placate internal audiences as well as to influence external parties. The lack of specific examples in the Amnpardaz report would appear to support this. However, it is worth noting that the published information is sufficient to develop fairly robust detection signatures that can identify potential samples of the iLO tool. At this time, at least one item has been identified matching the Amnpardaz report, so their analysis cannot be completely discounted. But the technical match does not automatically prove the targeting and potential intention

items that would make this capability uniquely focused on Iranian interests. Thus we should proceed with some degree of caution, even if available details indicate interesting possibilities may exist.

Overall, the iLO implant identified represents an interesting, if not necessarily completely unique, capability designed to perform disruptive activity in a very strange and uncommon fashion. While evidence to completely confirm (or deny) hypotheses around this event remains frustratingly lacking, the source and nature of disclosure strongly hint at additional motivations behind revealing this operation. With luck, the community will be able to gather more information (and ideally samples) related to this activity allowing for firmer disposition. Until that time though, security analysts and other interested parties will remain in a state of uncertainty – but also one of anticipation.