The ARC of Satori

arbornetworks.com/blog/asert/the-arc-of-satori/

by ASERT Team on January 18th, 2018
Authors: Pete Arzamendi, Matt Bing, and Kirk Soluk.

Satori, the heir-apparent to the infamous IOT malware Mirai, was discovered by researchers in December 2017. The word "satori" means "enlightenment" or "understanding" in Japanese, but the evolution of the Satori malware has brought anything but clarity. Each new version offers a fresh combination of targeted platforms, propagation techniques, and attack types. Contrasted with traditional software, in which features are added incrementally, Satori seems to go both forward and backward. Digging into the history will provide insight into this continually evolving threat.

A Short History of IOT Malware

Headlines about massive DDoS attacks first captured the public's attention on IOT security in late 2016. The malware responsible, Mirai, didn't target Windows machines like most threats – it targeted weaknesses in IOT devices and other embedded systems. These devices make great DDoS zombies, since often they run a stripped-down version of Linux, are directly connected to the Internet, and have limited security features. Mirai, and its many copycats, operate with similar principles:

- Propagation – Infected devices will attempt to infect other, randomly chosen, devices. Mirai started by using common username/password pairs via the antiquated telnet protocol. Later versions would use platform-specific vulnerabilities, like command-injection bugs in the web interface of home routers, to spread.
- Command-and-control – Once infected, the bot – in addition to propagating – would periodically check-in to a command-and-control site for updates and attack commands.
- Attack – Once instructed by the command-and-control, bots would launch a coordinated flood of attack traffic directed at the victim. This can be a flood of TCP packets with specific flags set, UDP packets, HTTP requests, or other more complicated attacks.

The authors of Mirai eventually published the source code to the malware. With it, anyone who knows how to use a compiler could setup their own command-and-control site and quickly build their own Mirai botnet. Those with more technical know-how could add features like new propagation methods, command-and-control protocols, and new attack types.

Satori

Researchers first discovered Satori in December 2017 and other versions of it have been identified since. The initially discovered version of Satori distinguished itself from Mirai in that its propagation method targeted two vulnerabilities in IOT devices – a "zero-day" in Huawei's home gateway and a previously-known command execution vulnerability in Realtek's UPNP SOAP interface. Both were clearly intended to target two very specific types of devices, unlike the more agnostic Mirai, which would infect any device with a default or easily guessable telnet username and password. Although there is evidence Satori re-used at least some of the public Mirai code, its precise targeting was what caught the eye of researchers. To perhaps further muddy the waters, other versions of Satori do indeed use telnet to propagate, but with a more sophisticated list of usernames and passwords. Every IOT malware including Satori is delivered to a victim in a compiled, ready-to-run format. That means a Linux executable compiled specifically for the architecture of the victim. For instance – an ARM device cannot run an executable compiled for x86 processors. Before delivering its payload, both Mirai and Satori poke and prod the victim to determine which pre-compiled version of the Mirai binary to download and execute. Satori raised the bar by introducing new architectures – superh and ARC. It's unclear whether the actors behind Satori did this because they knew a vulnerable population existed, or only hoped that it did. Below is a chart showing the similarities and differences, based on ASERT analysis, between the three most recent variants of Satori. Complementary information, including additional IoC's, can be found in [1]-[5]. Variant 1 is not included due to its lack of functionality as discussed in [1].

We distinguish the fourth variant of Satori, in part, because it appears to be the first known ARC malware. Adding the capability to run on the ARC chip set greatly expands the potential botnet population. According to [6], an article that was written in 2014, "ARC processor IP cores have been licensed by more than 190 companies and are used in more than 1.5 billion products a year." Furthermore, now that this new ground has been broken, it paves the way for other malware authors to target that architecture.

DDoS Mitigation

Since the variants of Satori all leverage different subsets of the Mirai DDoS attack codebase, longstanding Mirai-based DDoS mitigation advice still applies. See for example the ASERT Blog entitled Mirai IoT Botnet Description and DDoS Attack Mitigation [7]. Arbor customers can also obtain detailed Arbor product-specific mitigation advice by requesting the latest ASERT Mirai threat advisory from their account team or Arbor ATAC. Additionally, the continued expansion of DDoS-capable malware to different processor architectures further emphasizes the need for network operators to adopt network BCPs. While Mirai showed an affinity for IPTV cameras and DVRs with weak passwords, threat actors are rewarded for targeting devices others have not. As malware authors expand to ARC and other embedded processors, DDoS-capable malware can subvert a wider range of Internet-connected devices such as phones, gaming consoles, etc. Network operators must re-think their defensive strategies to also protect against compromised internal devices including those which can't be tracked down by following a cable. The collateral damage due to scanning and outbound DDoS attacks alone can be crippling if network architectural and operational best current practices (BCPs) are not proactively implemented. BCP references can be found at [8] and [9].

Conclusion

While the impact of IOT malware is self-evident, the threat landscape is constantly evolving. The weakest-of-the-weak, default usernames and passwords, have already been abused and attackers move on to more bountiful fruit – exploitable vulnerabilities in devices themselves. This reflects the harbinger that Mirai brought the world in 2016 – IOT devices are insecure and will be abused. We expect the three principles of IOT malware – propagation, command-and-control, and attacks – to remain the same, but become more sophisticated and evolved over time.

References

[1] https://researchcenter.paloaltonetworks.com/2018/01/unit42-iot-malware-…

[2] https://research.checkpoint.com/good-zero-day-skiddie/

[3] http://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spread…

[4] http://blog.netlab.360.com/early-warning-a-new-mirai-variant-is-spreadi…

[5] https://www.reddit.com/r/LinuxMalware/comments/7p00i3/quick_notes_for_o…

[6] http://www.techdesignforums.com/practice/technique/power-performance-pr…

[7] http://asert.arbornetworks.com/mirai-iot-botnet-description-ddos-attack…

[8] https://app.box.com/s/osk4po8ietn1zrjjmn8b

[9] https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

Posted In

- Attacks and DDoS Attacks
- Botnets
- Malware
- threat analysis

Subscribe

Sign up now to receive the latest notifications and updates from NETSCOUT's ASERT.