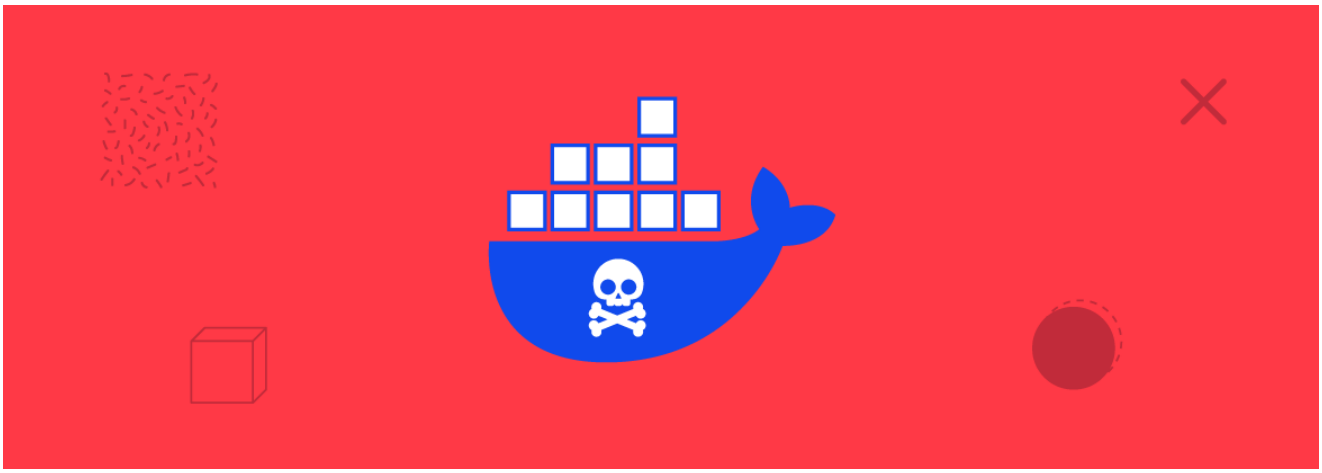
All About Doki Malware

securecoding.com/blog/all-about-doki-malware/

January 6, 2021

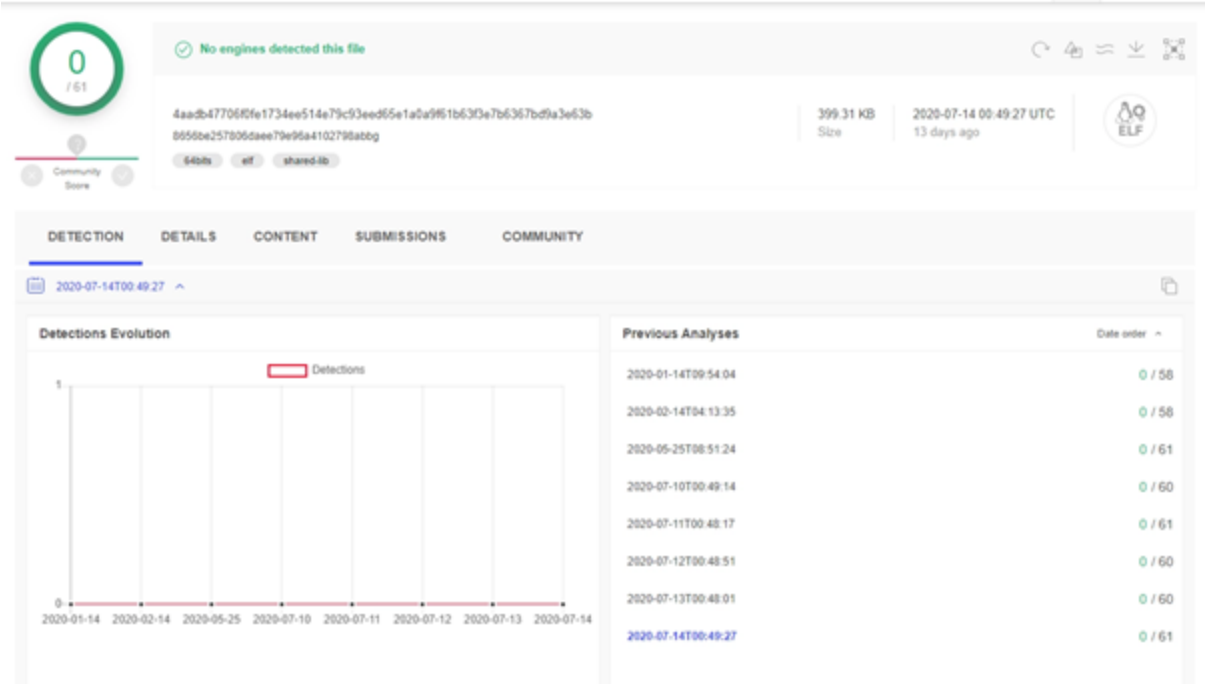
1 Like Unlike
January 6th, 2021



Software is as competent as the programmers who develop it. This has led to a world of marvellous and effective technologies across a wide spectrum of channels and media. It also leads along the way to the creation of software that is incredibly malicious, and in some cases quite dangerous.

We are talking about malware. Malware, or malicious software, is any device or directory which is harmful to the machine of a user. It is the standard term of a diverse range of malicious software types including viruses, ransomware, and spyware.

In the past several decades, almost everything has fundamentally changed when it comes to malware and malware analysis. Threats such as malicious software have been around for decades but during this period they were referred to as viruses. The Creeper virus from 1971, developed as a test by BBN Technologies engineer Robert Thomas, was among the first notable malware.



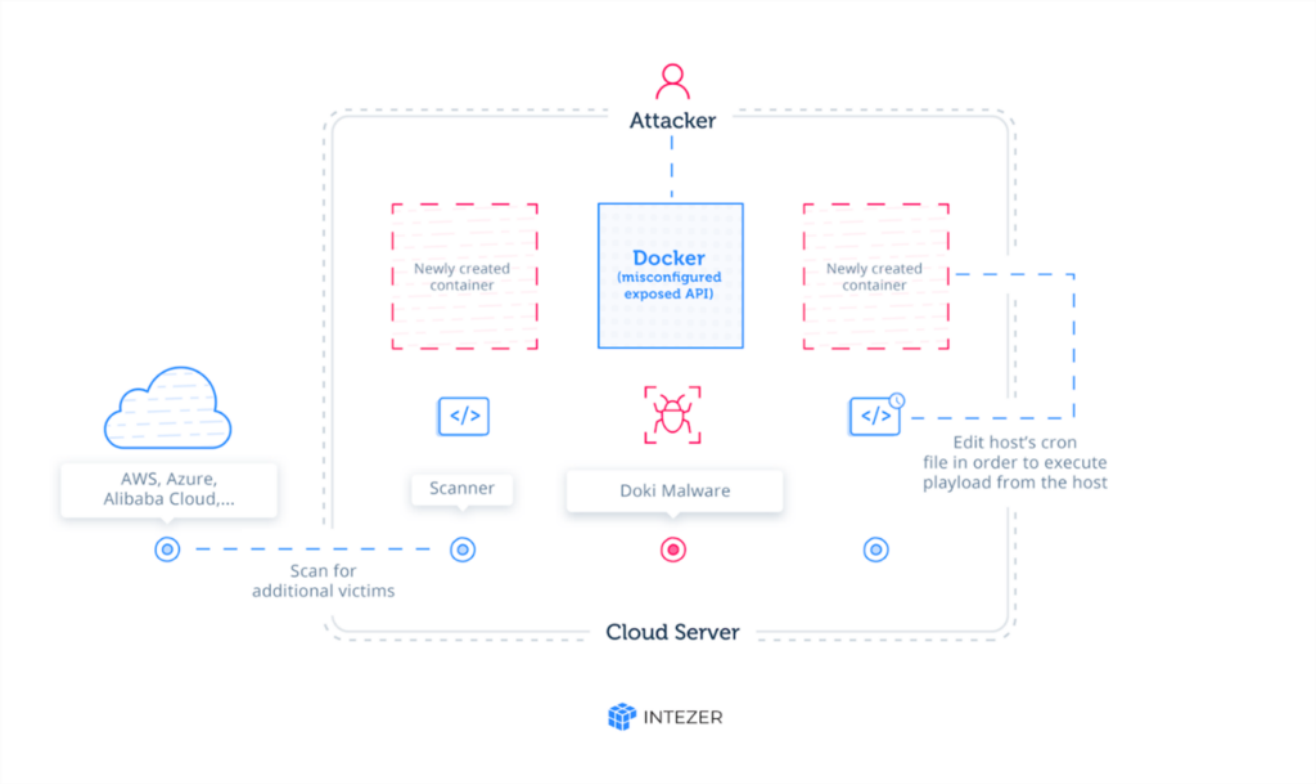
However, Yisrael Rada first introduced the term malware in 1990. Most of these early contagious programs were originally released as tricks or prototypes but attackers are now using malware to harvest corporate, financial, and private data.

Different forms of malware have distinct characteristics and functionality. These malicious programs may perform various functions, such as pilfering, intercepting or erasing confidential data, modifying or sabotaging fundamental computing functions, and tracking users' computer operations without their consent.

Doki Malware and Its Cause

Doki malware is a recent trojan that spreads via the Ngrok botnet using Dogecoin wallets for its C2. It targets publicly accessible Docker servers. Doki has been unrecognized for more than seven months as malware on VirusTotal, saying it is"an undetected backdoor."

According to Intezer cybersecurity researchers, Doki has a pervasive code-execution capability on a compromised server, gearing up for any variety of malware-based operations, from denial-of – service/subversion to data eavesdropping to malware.



Doki operates as an unnoticeable loophole for Linux, which constitutes an extension of the Ngrok Botnet program from two years ago. Disconcertingly, since it was first discovered in January 2020, it has also managed to avoid each of the 60 malware platforms identified on VirusTotal.

Doki uses a previously unrecognized approach to access its user by breaching the Dogecoin crypto-currency blockchain in a particular means to develop its C2 domain address remotely.

The vulnerability targets faulty containerized cloud systems. The hackers search for and manipulate publicly available Docker API terminals to mount their containers and deploy malware on the infrastructure of the perpetrators. Throughout that attack, the intruders revive and delete several containers.

Every container produced during the attack is predicated on an alpine image configured with curl. The image on the Docker platform is not malevolent, but to perform malicious activities it is being misused. Curl commands are implemented using a curl application picture as soon as the container is likely to launch.

Prevention

Higher security hygiene and stipulations designed especially for container conditions can defeat Doki.

Step 1

Doki sets off their invasion by searching a network for a poorly configured port of the Docker API. The attacker calls the Docker API to cause a request and open a clean container after they have identified a Docker port to manipulate. Security testing engines won't find any problems with this. Before the attack escalates, it is a test site.

Attackers will use the containers they are manipulating to build more containers easily to cause any suspicious attacks. Doki creates a command-and-control connection, using the ngrok tunneling tool. Several specific short-lived URLs allow attackers to quickly download payloads into the file server of the container.

Step 2

When logs are gathered and warnings are sent, the container is gone without a hint. By linking the host root file system the attack container uploads the host system. Then it modifies the cron functionality and achieves resources for host execution. Typical of container attacks, the malicious application may try to return to the host once an entitled container is managed.

Step 3

The attack creates a host cron job with a network detector and a plugin script that implements every minute a malicious script. Using a list of public domain IP ranges, the network scanner scans for another target.

Step 4

This Doki malware will function as a container or as a server, and can easily be scaled up. Doki requests the Dogecoin API, uses SHA265 protection and generates a run-time URL address interactively. This bypasses network infrastructure security screening like the URL / IP blacklist lists.

Conclusion

"Doki" is a complex malware attack that exploits the current Docker architecture to strike, exploit, and distribute the architecture. To detect and block complex links, unwanted process/file operation, and privilege incursions, modern container and cloud infrastructures need similarly contemporary information security.

The Doki malware is lightweight and unchanging, taking just several minutes to afflict and ramp up an attack. Runtime containers and host teams consisting of manufacturing environments are the most important protections to combat Doki (and subsequent attacks that have come and will come) before they can cause mayhem.