DUKU

STUXNET'S NEW AVTAAR!

Few months back world has experienced the devastative nature of Stuxnet and today Duku, a malware, like stuxnet has alerted this subcontinent with its arrival.

With the Command and Control server for Duku based in India and the IP address is being blocked by the ISP, a Stuxnet like malware is finally here. It is named "Duqu" as the infection created files with DQ were used. An analysis of the executables of Duku has startled the Malware researchers due to its similarities with the Stuxnet binaries. However, Duku comes with more security features and encrypted communications. Unlike Stuxnet which had payload for SCADA/PLC systems, 0 day exploits for delivery of the infection, Duku, has the same codebase as that of Stuxnet but doesn't have SCADA/PLC related codebase. A C&C server was incorporated into the code of Stuxnet as an added feature.

Researchers are analyzing the vulnerabilities, which are being exploited, but primarily Duku is functional as a RAT (Remote Access Trojan). It was a highly targeted attack on specific organizations for specific assets. This was for reconnaissance purposes and various types of data-files were collected and uploaded to the C&C server, probably to launch another offensive attack specifically targeting these assets. Mode of delivery is still unknown, however the information stolen was related to keystrokes, network shares passwords

and loads of other features as mentioned below:

a. List of running processes, account details, and domain information
b. Drive names and information, including those of shared drives
c. Take a screenshot
d. Network information (interfaces, routing tables, shares list, etc.)
e. Keylogger
f. Window enumeration
g. Share enumeration
h. File exploration on all drives, including removable drives
i. Enumerate computers on the domain through NetServerEnum

Since there are similarities in the code base with the Stuxnet code, either it is the handiwork of Stuxnet authors, or by those who have access to the source code of Stuxnet. However, SCADA/PLC related code is missing from Duku, which is a huge relief, as of this moment.

Researchers have found infections; however have been unable to lay their hands on the Dropper Application, which is responsible for the delivery of the secondary payload i.e. the infection.

Since, a lot of time has been utilised by developers of Duku, the probable sources can be phishing mails, USB, network shares. Out of the various methods available, which method has been utilised to drop the binaries will define the exact purpose and intention of the authors.

Let us talk about a few examples of Attack vector mapping. It is used to derive a relationship between the type of attack and the methods utilised for deployment of these attacks.

Let us say, for example a malware is propagating via network shares. Therefore, the general conclusion is that this malware is used for a targeted attack on a particular entity. This entity can be a corporate or a home user, however the payload may vary. Other examples are as follows:

- Spear Phishing — email with attachments — targeted attack
- Drive by downloads — mass attacks mostly deployment of Botnets or stealing personal information
- SQLi — Injecting JS in multiple sites — exploit, download and execute to infect — Botnets or stealing personal information

In this scenario, according to the primary research paper, certain European organizations were targeted and since the code was very much similar to Stuxnet. In all probability, it would not come as a surprise to us if these targeted companies were in anyway related to Siemens. Secondly, the mode of delivery would have been a Spear Phish email. Since most of the Anti-Viruses have now disabled the autorun for the USB drives, which effectively means the probability of USB based propagation decreases drastically.

Malware Authors have a strange way of inserting their motives, or identity. A Russian malware author inserted his car's number plate, while the writers of the Brain virus inserted their address. In the case of Duku, researchers have found a part of a JPEG file, which was originally from Nasa's Hubble Imagery section — portraying the merger of galaxies, i.e. when two galaxies collide.

If we let our imagination run wild, then maybe they want to tell the whole world that, Duku is a by-product of a merger of two different entities/ ideologies.

Duku was designed with a lifespan of 36 days after which it is supposed to remove itself from the system. This conforms to our belief that we should expect another wave of attack in the near future based on the information, which has been stolen and can be more devastating than Stuxnet.

There is no reason, which we can think of the 36-day limit. However surely, it has to do with conducting the recee of the systems, networks and AV detection or maybe they are inspired by lyrics of "36 Days" by Hawk Nelson.

"Now I'll sing with all this is within me
After thirty-six days on the road"

In addition, a question arises that why the code of Stuxnet has been used to steal the information, when there are already many options of info stealing malware with their source-code readily available. From a software developer's point of view, it is easy to modify the existing codebase to suit the upcoming requirements/changes rather than incorporating these changes in a different codebase.

This attack also acts as a learning experience for the authors of Duku to:

1. Gauge the AV detection rates for the present code and incorporate changes in the codebase vis'a'vis the AV evasion techniques
2. IT preparedness of the infected organizations
3: Fine tuning of the Delivery mechanism

This attack would also aid the authors of Duku in procuring more certificates for code signing or other nefarious purposes. If Stuxnet was rumoured to have been designed to pull down Iran's Nuclear program, most of the Duku researchers are still wondering who would it be next.

This was a recon attack with the purpose to steal system and network information and most probably the latest developments by these infected organizations. The amount of information that had reached its intended recipient is still unknown.

Researchers are not even aware if any of the digital certificates were stolen. In the past, we have seen Diginotar and Comodo being hacked and fake certificates were generated. In the case of Stuxnet and Duku, we have seen valid certificates being used for signing the code.

Hence, we in India expect in near future from Duku Deux, which may not target these organizations but the products developed by these organizations, might be at risk.

In addition, we expect in the near future from Duku Deux:

1. AV evasion encoding
2. More stolen Certificates will be revealed
3. PLC attack or No PLC attack - only time will tell.

—By: MR. Govind Rammurthy, MD & CEO, eScan.