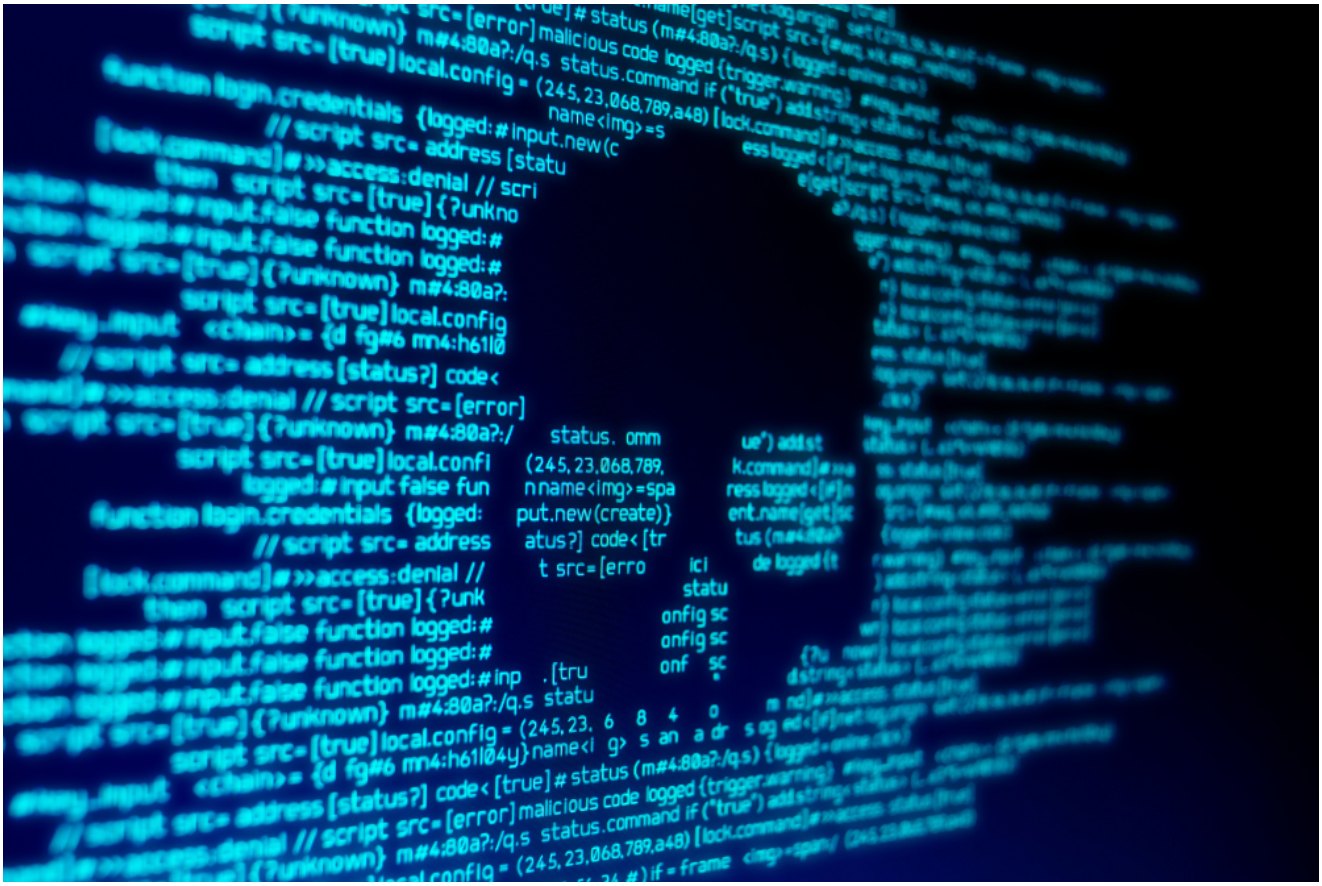
New Satan ransomware variant ‘Lucky’ exposes 10 server-side vulnerabilities

cyware.com/news/new-satan-ransomware-variant-lucky-exposes-10-server-side-vulnerabilities-070afbd2



- Satan ransomware resurfaces with a new variant named Lucky, exploiting multiple application vulnerabilities that affect both Windows and Linux-based servers.
- Attackers are evolving towards server-side exploits.

Since the first discovery of Satan ransomware back in early 2017, it has surfaced multiple times, exposing new vulnerabilities. It began with a unique model of Ransomware as a Service (RaaS) which enabled any cybercriminal to create a customized version of the Satan Ransomware.

It resurfaced again in 2018 by adding EternalBlue and Mimikatz exploits to its arsenal. In previous versions, the ransomware targeted vulnerabilities that primarily affected the Windows operating system. However, in its latest iteration now, it has exploited 10 server-side vulnerabilities which affect both Linux and Windows systems.

This new variant of Satan ransomware, dubbed Lucky, was spotted by security vendor NSFocus in November 2018. NSFocus reported that Lucky spreads itself by exploiting several application vulnerabilities affecting Windows services, Apache Tomcat, JBoss, WebLogic, Springs, and Apache Struts.

Lucky spreads primarily like a worm but does not perform any obviously malicious actions on the infected machines, apart from encrypting the target files. Lucky was also found by Sangfor Tech, which discovered the ransomware in one of its financial sector customer's Linux servers. Sangfor Tech found that the ransomware encrypts files and appends '.lucky' to the name of the encrypted files.

Despite a decline in major ransomware activity in 2018, as compared to the WannaCry and NetPetya attacks seen last year, ransomware still remains a danger for the owners of online services, with an increasing number of server-side exploits.

Evolution of Satan

As seen in the case of Satan and other ransomware threats, attackers have changed their strategy from primarily targeting operating system vulnerabilities to targeting server-side vulnerabilities. This shift could have an even bigger impact.

Apostolos GIannakidis, from Waratek, told Dark Reading that one of the reasons for this shift in strategy could be the fact that patching servers and mitigating the effects of ransomware attacks on servers is more time-consuming and can result in downtime for the affected online services.

Mitigations

One of the major reasons behind the exposure of servers is that many servers often use an older version of applications or libraries, which remain vulnerable to previously discovered exploits. Therefore, it is essential for owners of any affected web servers to upgrade all the applications which are targeted by Lucky ransomware.

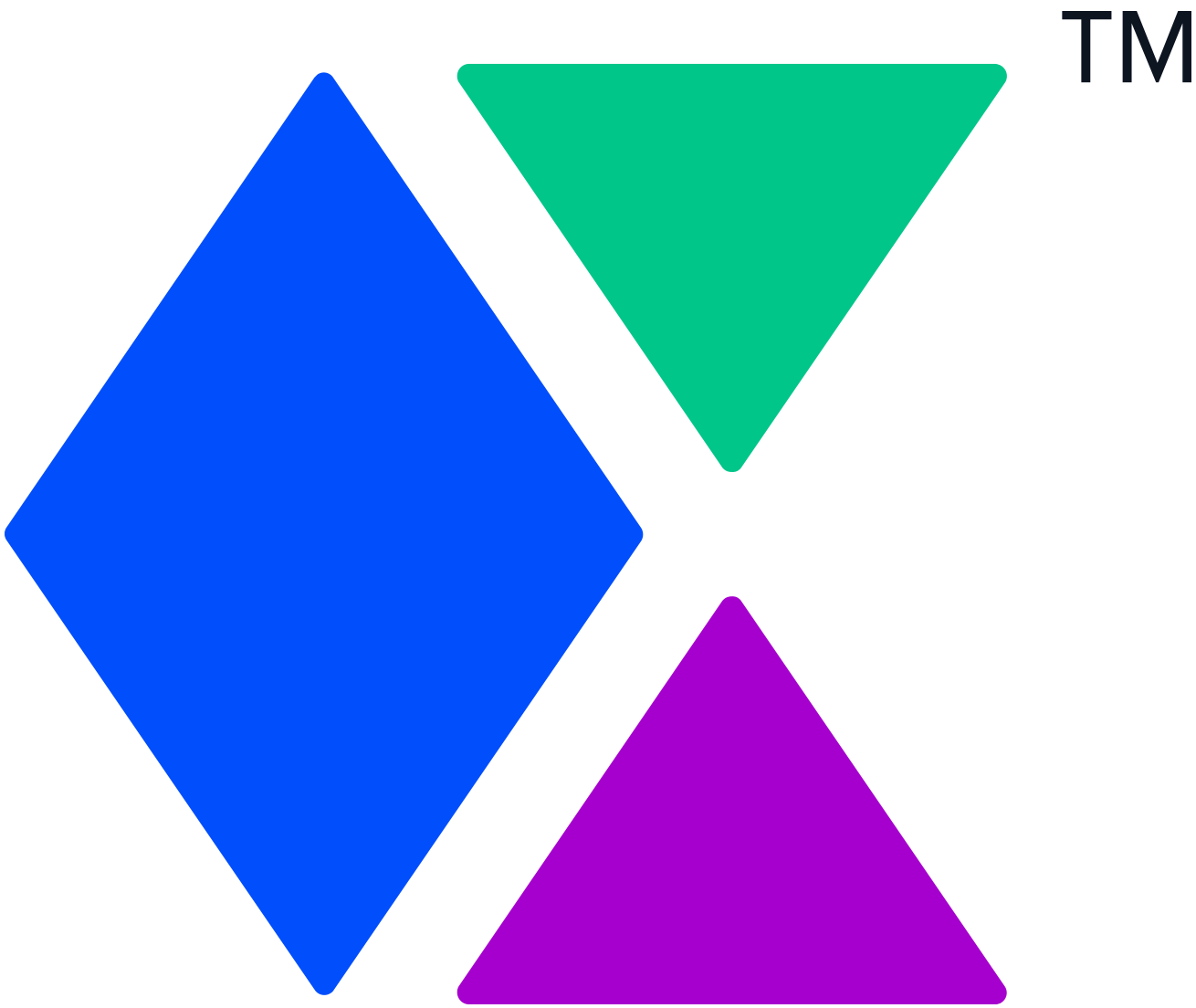
Furthermore, Lucky also exploits vulnerabilities in Windows OS services, which means that the owners also need to install the necessary patches to avoid an attack. The complete list of the patches and upgrades necessary for the remediation are provided by NSFocus in their blog post.

Apart from these, it is important to always follow the industry best practices when maintaining any online services. These include:

- Changing default admin account usernames and using complex passwords.
- Using the latest security solutions to defend against future attacks.
- Isolation of critical network elements from the rest of the network to prevent the spread of ransomware.

- Training employees for an effective threat response in case of any attacks.
- Backing up critical data periodically to avoid any data loss.

NSA EternalBlue Exploit | Ransomware Attacks | Satana Ransomware | Mimikatz



Publisher

Cyware