2020

[Trickbot & Anchor_DNS]

FS-ISAC

KORI YOUNGER

Anchor DNS:

The developers of TrickBot created anchor_dns, a DNS tunnel, as a new tool to send and receive information from the victims' machine. Trickbot, a popular banking trojan, acts as a trojan horse for other malware.

Anchor_dns was first observed in early 2019. Anchor_dns acts as a backdoor that allows victims machines to send and receive data through communication with command-and-control (C2) servers over DNS. This communication enables attackers to bypass typical network defense products by merging the attack patterns with regular, legitimate DNS traffic.

Anchor_dns is deployed on a victim's device after visiting one of the listed malicious domains. Victims typically access this domain through a link sent via a phishing email. Mangoclone.com is just one of four outbound domains tied to the Anchor_DNS attacks. kostunivo.com, chishir.com, and onixcellent.com are among the other domains associated with anchor_dns. These domains are hosted on servers with the following IP addresses 23.95.97.59, 51.254.25.115, 193.183.98.66, 91.217.137.37,87.98.175.85. Anchor_dns uses a single-byte XOR cipher to encrypt its communications, meaning the anchor_dns string is only detected once decrypted.

Indicators of Compromise:

The malware copies itself onto one of 3 directories in an infected hosts' system, C:\\Windows, C:Windows\SysWOW64, or C:\Users\<username>\AppData|Roaming, naming the executable file as 8 random characters (ex: adbcdefgh.exe).

Every 15 minutes, the malware runs scheduled tasks to maintain persistence on a host. These tasks use common naming conventions comprised of a folder located in %APPDATA% and autoupdate# followed by another random series of 5 numbers. The malware then deploys more malicious batch scripts using PowerShell commands. Once this is done the malware will execute self-deletion using PowerShell commands cmd.exe /c timeout 3 && del C:\Users\<username>\<malware_sample> or cmd.exe /C PowerShell \"Start-Sleep 3; Remove-Item C:\Users\<username>\<malware_sample_location>\".

Mitigation:

The first step to mitigating risk is implementing network or host-based DNS blocks of the 4 known malicious domains and 5 IP addresses of the C2 servers for all DNS traffic. Then, security staff is advised to analyze the network for indicators of compromise to block the attack as early as possible. Typically, this would be done by searching for the malicious file name. However, the randomized naming of these files makes this a

difficult task. In some cases, the malware will leave behind a anchorDiag.txt file that may be a legitimate IOC.

Depending on security tools used by the organization threat hunters may be able to identify an IOC by finding scheduled task matches for "autoupdate#". Security teams are also urged to locate self-deletion commands. Best practices include investigating any and all results and adding the previously mentioned signals to all threat response tools for continuous monitoring.

In the event of a positive IOC administrators should immediately backup and secure sensitive data and maintain all logs and follow common best practices for mitigating a ransomware attack.

Targets to the Finance Sector:

Anchor_dns has been noted to target victims with valuable financial information. The malicious actor can deploy remote administration tools and may deploy malware of any type, making the threat associated with anchor_dns virtually infinite. Reported cases of anchor_dns attacks have indicated a prevalence of POS malware and ransomware. POS malware is used to steal sensitive information, including credit card information affecting consumers as well as the reputation of corporations in the event of a large data breach.

Sources:

CISA Alert (AA20-302A)

FS-ISAAC_Ransomware2020