Chinese hackers use ransomware as bait to hide cyber espionage

Two Chinese hacker groups are carrying out cyber espionage campaigns and stealing intellectual property from Japanese and Western companies. To cover up their espionage, these groups of hackers pretend they're spreading ransomware.

Threat analysts from Secureworks share that hackers use ransomware in espionage activities to erase their tracks and create a distraction for employees dealing with cybersecurity incidents.

Finally, the theft of business secrets is disguised as extortion attacks.

Strange ransomware campaigns

Two hacking campaigns analyzed by Secureworks are "Bronze Riverside" (conducted by hacker group ATP41) and "Bronze Starlight" (ATP10), both of which use HUI Loader to deploy remote access trojans PlugX, Cobalt Strike and QuasarRAT.

Starting in March 2022, "Bronze Starlight" leveraged Cobalt Strike to deploy ransomware families such as LockFile, AtomSilo, Rook, Night Sky, and Pandora.

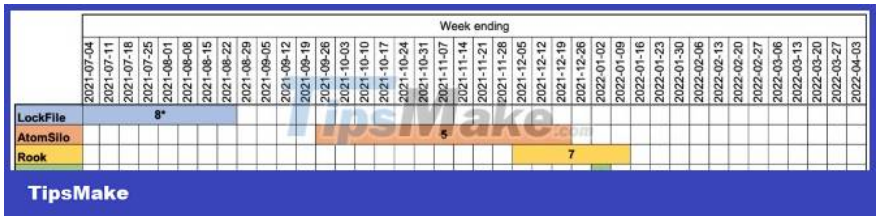
In these attacks, hackers use a new version of HUI Loader with the ability to bridge Windows API calls and the ability to disable Event Tracing for Windows (ETW) and Antimalware Scan Interface (AMSI).

Cobalt Strike configuration for three separate ransomware AtomSilo, Night Sky and Pandora reveals a shared C2 (Command & Control server) address. Also, this year the same source uploaded to the HUI Loader on Virus Total.

Cobalt Strike C2 domain	HTTP POST URI	Ransomware
update . ajaxrenew . com	/rest/2/meetingsVDcrCtBuGm8dime2C5zQ3EHbRE156AkpMu6W	AtomSilo
api . sophosantivirus . ga sub . sophosantivirus . ga	/rest/2/meetingsQpmhJveuV1IjApIzpTAL	Night Sky

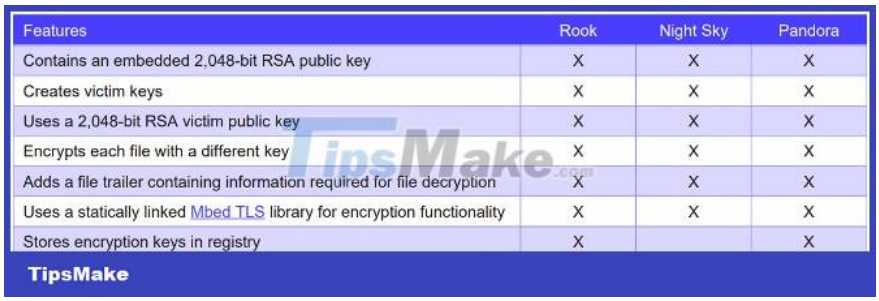
TipsMake

The way LockFile, AtomSilo, Rook, Night Sky and Pandora work and victims are very unusual compared to purely financially motivated ransomware campaigns. Often they target a small number of victims for a short time and then suddenly abandon the campaign.



Secureworks also recognizes that there is code duplication between Pandora and the HUI Loader so this loose connection could point to a common pool.

LockFile and AtomSilo also look very similar while Night Sky, Pandora and Rook are all built from Babuk source code and also have many similarities in code.



Features	Rook	Night Sky	Pandora
Contains an embedded 2,048-bit RSA public key	X	X	X
Creates victim keys	X	X	X
Uses a 2,048-bit RSA victim public key	X	X	X
Encrypts each file with a different key	X	X	X
Adds a file trailer containing information required for file decryption	X	X	X
Uses a statically linked Mbed TLS library for encryption functionality	X	X	X
Stores encryption keys in registry	X		X

These 5 ransomware campaigns left no mark on the cybercriminal community and never really became a significant threat. In addition, all of them were soon abandoned.

Therefore, it can be said that "Bronze Starlight" is creating short-lived strains of ransomware to mask cyber espionage activities, disguised as a ransomware attack.

In response, Secureworks recommends that organizations and businesses strengthen their ransomware detection and protection mechanisms. At the same time, when detecting ransomware, organizations and businesses should thoroughly check other aspects in parallel with ransomware removal.