SentinelLABS

Background

features and under-the-hood elements with its predecessors. However there have been a few key updates, including tweaks to encryption, methods of exfiltration, and the (now commonplace) use of a public “leak blog” to post victim data for those who do not comply with the ransom demand.

Evolution of Ranzy Ransomware

At its heart, Ranzy is a RaaS (Ransomware as a Service) offering. Payloads are typically distributed via email (phishing), although there are some reports of delivery via the web (drive-by downloads). The “rebrand” from ThunderX to Ranzy occurred after free-decryption programs for ThunderX started to appear. A free decryption tool for ThunderX was posted to the NoMoreRansom project in September of this year.

This ‘rebrand’ distances the actors from ThunderX as well as improves upon the encryption mechanism so as to reduce the feasibility of future, free, decryption tools. With ThunderX emerging around August 2020, it would seem as though the lifecycle of this particular family has been rather short throughout its evolution. Note that some early samples of Ako were observed around January 2020.

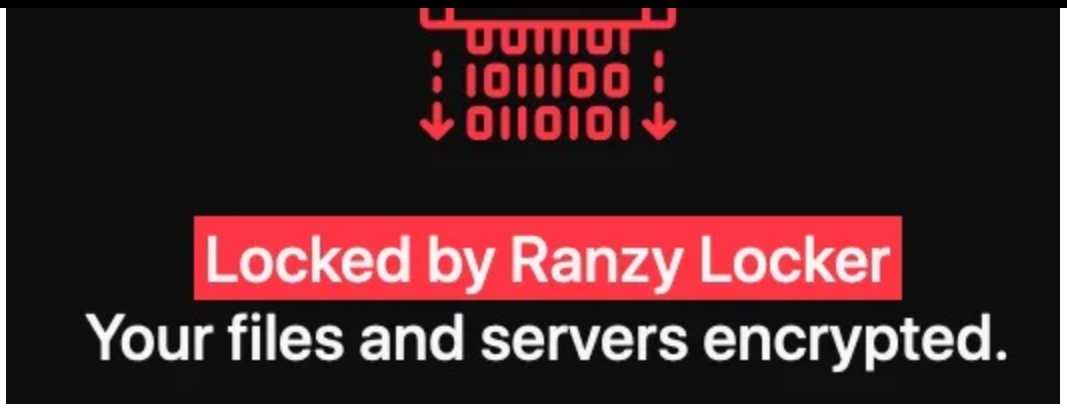
1.1) append a `.ranzy` extension to encrypted files (with early versions using just `.RNZ`). Also of note, current Ranzy Locker payloads tend to include the same PDB patch as their ThunderX ancestors:

```
C:UsersGh0StDesktopThunderXReleaseLockerStub.pdb
```

Improved Encryption Routines

Ranzy uses a combination of encryption algorithms to affect targeted data. An embedded RSA-2048 key is built into the ransomware payloads, with Salsa20 being utilized for specific file/data encryption. Ranzy contains functionality to locate and encrypt additional local drives (`GetLogicalDrives`), as well as adjacent (and accessible) network drives (`NetShareEnum`).

Ranzy, like ThunderX and Ako, will attempt to encrypt multiple file types by extension while excluding specific extensions and/or paths based on strings. Files that do not contain the `.dll`, `.exe`, `.ini`, `.lnk`, `.key`, `.rdp` are subject for inclusion. The ransomware will also exclude specific critical paths with strings including **AppData**, **boot**, **PerfLogs**, **PerfBoot**, **Intel**, **Microsoft**, **Windows** and **Tor Browser**.



Once launched, Ranzy payloads take a number of steps in order to both ensure maximum impact (encryption) as well as inhibiting standard recovery options where possible. Specific commands, and syntax, can vary across Windows versions and flavors. This includes the use of standard system tools to manipulate VSS and boot time recovery options.

After execution, the ransomware will swiftly call WMIC.EXE with the following syntax:

```
wmic.exe SHADOWCOPY /nointeractive
```

The following WBADMIN, BCDEDIT, and VSSADMIN commands are then issued to shift the victim host to the desired, compromised, state:

```
wbadmin DELETE SYSTEMSTATEBACKUP
wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest

bcdedit.exe /set {default} recoveryenabled No
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
```

terminating any problematic process standing in the way of encryption or further manipulation of target systems. It is not uncommon for explorer.exe or other running processes to quickly exit and relaunch once Ranzy's process begins.

Both Ranzy versions analyzed appear to retain the same multithreading capabilities that first appeared in ThunderX. The payload will first identify the number of processors available via `GetSystemInfo()`. Following this, the ransomware will leverage `IoCompletionPort` to generate a queue of files which are to be encrypted. Then, the ransomware is able to allocate a number of threads (equal to 2x the count of processors identified). This allows for fairly competitive (and therefore dangerous) encryption speeds when compared to the likes of Maze or NetWalker.

Post Encryption Behavior

Ranzy's ransom notes are deposited into each folder containing affected files/data. Across the analyzed versions, these are always identified with the name **readme.txt**. There are minor variations in the ransom notes across versions of the ransomware. That being said, the basic structure and content across ThunderX, Ranzy and Ranzy 1.1 are all quite similar.

Examples of the Ranzy and Ranzy 1.1 ransom notes can be seen below.

instructions and “support” (live chat). Previous variations simply instructed victims to reach out via email for further instructions.

Non-compliant victims are currently being cataloged on the group’s blog, entitled “Ranzy Leak”. As of this writing there are 3 victims listed on the site, representing the electrical engineering, security & investigations, and Government administration industries.

Conclusion

The Ranzy, ThunderX and Ako family is yet another example of how nimble and aggressive these threats and the actors behind them are becoming. With little to no barrier for entry (beyond a small investment of cash), any enterprising cybercriminal can gain access to, and manage, ransomware like Ranzy, potentially causing a great deal of financial damage. As we know, this damage is not limited to the direct payment of the ransom (which you should avoid), but now also includes any penalties associated with data breaches, public posting of private data, GDPR / compliance fallout, and beyond.

These threats are very agile, and it is clear that the actors behind them are paying attention to the efforts on the defense side. For example, when decryptor utilities are released, they quickly update their code and start distributing better and stronger payloads to nullify any workarounds.

Indicators of Compromise

393fd0768b24cd76ca653af3eba9bff93c6740a2669b30cf59f8a064c46437a2

90691a36d1556ba7a77d0216f730d6cd9a9063e71626489094313c0afe85a939

bbf122cce1176b041648c4e772b230ec49ed11396270f54ad2c5956113caf7b7

ade5d0fe2679fb8af652e14c40e099e0c1aaea950c25165cebb1550e33579a79

SHA1

43ccf398999f70b613e1353cfb6845ee09b393ca

35a663c2ce68e48f1a6bcb71dc92a86b36d4c497

38b86dacb1568af968365663c548bd9556fe0849

20102532dfc58bc8256f507da4a177850f349f7a

9a77e2f8bf0da35f7d84897c187e3aff322f024d

MITRE ATT&CK

Indicator Removal on Host: File Deletion T1070.004

Modify Registry T1112

Query Registry T1012

System Information Discovery T1082

Peripheral Device Discovery T1120

Inhibit System Recovery T1490

Create or Modify System Process: Windows Service T1031

Exfiltration TA0010

RAAS RANSOMWARE

JIM WALTER

Jim Walter is a Senior Threat Researcher at SentinelOne focusing on evolving trends, actors, and tactics within the thriving ecosystem of cybercrime and crimeware. He specializes in the discovery and analysis of emerging cybercrime "services" and evolving communication channels leveraged by mid-level criminal organizations. Jim joined SentinelOne following ~4 years at a security start-up, also focused on malware research and organized crime. Previously, he spent over 17 years at McAfee/Intel running their Threat Intelligence and Advanced Threat Research teams.

PREV

Resourceful macOS Malware Hides in Named Fork

NEXT

Egregor RaaS Continues the Chaos with Cobalt Strike and Rclone

RELATED POSTS

Xeon Sender | SMS Spam Shipping Multi-Tool Targeting SaaS Credentials

AUGUST 19 2024

NullBulge | Threat Actor Masquerades as Hacktivist Group Rebelling Against AI

JULY 16 2024

Search ...

SIGN UP

SentinelLABS

RECENT POSTS

Cloud Malware | A Threat Hunter's Guide to Analysis, Techniques and Delivery

OCTOBER 24, 2024

China's Influence Ops | Twisting Tales of Volt Typhoon at Home and Abroad

OCTOBER 16, 2024

Kryptina RaaS | From Unsellable Cast-Off to Enterprise Ransomware

SEPTEMBER 23, 2024

LABS CATEGORIES

Crimeware

Security Research

Advanced Persistent Threat

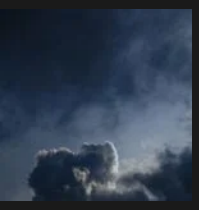
Adversary

SentinelLABS

SENTINELLABS

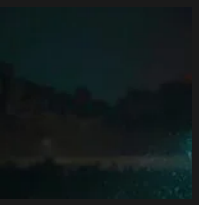
In the era of interconnectivity, when markets, geographies, and jurisdictions merge in the melting pot of the digital domain, the perils of the threat ecosystem become unparalleled. Crimeware families achieve an unparalleled level of technical sophistication, APT groups are competing in fully-fledged cyber warfare, while once decentralized and scattered threat actors are forming adamant alliances of operating as elite corporate espionage teams.

RECENT POSTS



Cloud Malware | A Threat Hunter's Guide to Analysis, Techniques and Delivery

OCTOBER 24, 2024



China's Influence Ops | Twisting Tales of Volt Typhoon at Home and Abroad

OCTOBER 16, 2024

SentinelLABS

SIGN UP

Get notified when we post new content.

Business Email >

Twitter LinkedIn