

## 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:

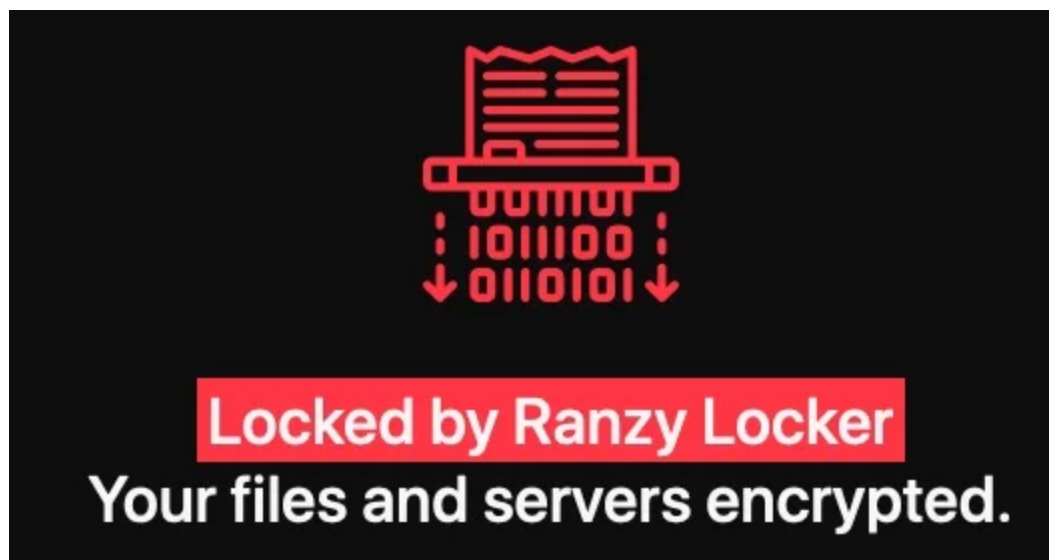
`C:\Users\Gh0st\Desktop\ThunderXReleaseLockerStub.pdb`

```
4786
4787     uStack4 = 0x54;
4788     local_64 = (void *)0x0;
4789     local_60 = 0;
4790     local_5c = 0;
4791     local_8 = 0;
4792     local_58 = param_1;
4793     DVar1 = GetLogicalDrives();
4794     uVar2 = 0;
4795     do {
4796         local_58 = (void *)0x104;
4797         local_54 = uVar2 + 0x41 & 0xffff;
4798         local_20 = (WCHAR)local_54;
4799         local_1c = 0;
4800         local_1e = 0x3a;
4801         FUN_00403437(local_38, (void *)0x104);
4802         lpRemoteName = (undefined8 *)local_38;
4803         if (7 < local_24) {
4804             lpRemoteName = local_38[0];
4805         }
4806         WNetGetConnectionW(&local_20, (LPWSTR)lpRemoteName, (LPDWORD)&local_58);
4807         FUN_00406a49((short **)local_38);
4808         FUN_00403401(local_50, (undefined8 *)local_38);
4809         FUN_00403715(local_38);
4810         local_8._0_1_ = 1;
4811         if (local_40 == 0) {
4812             if ((DVar1 & 1 << ((byte)uVar2 & 0x1f)) != 0) {
4813                 FUN_00403740(local_50, (undefined8 *)&local_54, (void *)0x1);
4814                 FUN_0040438b(local_50, (undefined8 *)&DAT_0041d598, 2);
4815                 goto LAB_00406b85;
4816             }
```

## Improved Encryption Routines

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.

```
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
```

```
vssadmin.exe Delete Shadows /All /Quiet
```

Ranzy Locker makes use of the Windows ‘[Restart Manager](#)’ API to assist in 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.

```
5527     local_60 = param_1;
5528     iVar1 = RmRegisterResources(local_50,1,&local_60,0,0,0,0);
5529     if (iVar1 == 0) {
5530         local_54 = 0;
5531         local_58 = 0;
5532         pvVar2 = (void *)0x0;
5533         local_5c = 0;
5534         uVar3 = 0;
5535         do {
5536             iVar1 = RmGetList(local_50,&local_58,&local_54,pvVar2,&local_5c);
5537             if (iVar1 == 0) {
5538                 if (local_5c == 0) {
5539                     RmShutdown(local_50,0,0);
5540                 }
5541                 break;
5542             }
5543             if (iVar1 != 0xea) goto LAB_004077d9;
5544             local_54 = local_58;
5545             if (pvVar2 != (void *)0x0) {
5546                 thunk_FUN_0040c5cd(pvVar2);
5547             }
5548             pvVar2 = (void *)FUN_004088c6(-(uint)((int)((ulonglong)local_54 * 0x29c >> 0x20) != 0) |
5549                                     (uint)((ulonglong)local_54 * 0x29c));
5550             bVar4 = uVar3 < 3;
5551             uVar3 = uVar3 + 1;
5552         } while (bVar4);
5553         if (pvVar2 != (void *)0x0) {
5554             thunk_FUN_0040c5cd(pvVar2);
5555         }
5556         if (local_50 != -1) {
5557             RmEndSession(local_50);
5558         }
5559     }
```

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

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.

Perhaps the most significant difference between the ransom notes is with Ranzy 1.1, victims are instructed to access a TOR-based portal for payment, further 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

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

### SHA256

c4f72b292750e9332b1f1b9761d5aefc07301bc15edf31adeaf2e608000ec1c9  
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](#)



Inhibit System Recovery [T1490](#)

Create or Modify System Process: Windows Service [T1031](#)

Exfiltration [TA0010](#)

RAAS

RANSOMWARE

## SHARE



### 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.



Resourceul macOS  
Malware Hides in Named  
Fork

Egregor RaaS Continues  
the Chaos with Cobalt  
Strike and Rclone

## RELATED POSTS

---

**Kryptina RaaS | From Unsellable Cast-Off to Enterprise Ransomware**

 SEPTEMBER 23 2024

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

 AUGUST 19 2024

Search ...



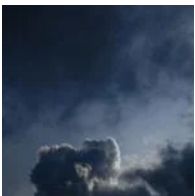
## SIGN UP

---

Get notified when we post new content.

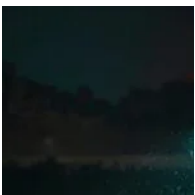
## RECENT POSTS

---



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



## LABS CATEGORIES

Crimeware

Security Research

Advanced Persistent Threat

Adversary

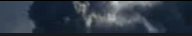
LABScon

Security & Intelligence

## 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



## 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



SIGN UP

Get notified when we post new content.

Business Email



Twitter



LinkedIn