Ranion Ransomware - Quiet and Persistent RaaS

September 30, 2021

Threat Research

By Shunichi Imano and Fred Gutierrez | September 30, 2021

FortiGuard Labs Threat Research Report

Many thanks to Val Saengphaibul who contributed to this blog.

Affected platforms: Microsoft Windows
Impacted parties: Windows Users
Impact: Encrypts files on the compromised machines and demands ransom from the victim to recover the encrypted files.
Severity level: High

Ranion is a Ransom-as-a-Service (RaaS) that has enjoyed unusual longevity as it has been active since at least February 2017. While its activities and purpose—encrypting files on compromised machines and receiving ransom payment from the user to recover their files—may seem the same as other ransomware in the public's eyes, the truth is that the inner workings of Ranion RaaS are unlike other ransomware.

In this blog, FortiGuard Labs will explain how Ranion RaaS works.

The opening lines of The Tale of Heike, a martial epic about the civil war between the Taira and Minamoto clans in 12th-century Japan, help describe the rise and fall of various ransomware groups in 2021.

"The Jetavana Temple bells
ring the passing of all things.
Twinned sala trees, white in full flower,
declare the great man's certain fall.
The arrogant do not long endure:
They are like a dream one night in spring.
The bold and brave perish in the end:
They are as dust before the wind."
— ***Royall Tyler, The Tale of the Heike***

Ransomware Operations are Short-Lived

For those of us monitoring cybercriminal organizations and malware, ransomware often has a very short shelf life. Some of the most notable ransomware movements in 2021 include:

Disappearance:

- The REvil (aka Sodinokibi) gang that had been active since 2019 went dark in June.
- The Avaddon ransomware group halted its operations in June. It had begun its operations in 2019.
- The Ragnarok ransomware gang, in operation since 2019, shut itself down in August and released its decryption key.
- Darkside first appeared in 2020 and closed in May after compromising a major US pipeline company.
- FonixCrypter ransomware gave up its criminal life in January and released a decryption tool and its master decryption key. The master decryption key can decrypt all files, regardless of the victim, that had previously been encrypted by FonixCrypter.

Debut and Rebranding:

- Ads for Blackmatter ransomware went up on cyber underground forums in July. While Blackmatter is not a rebrand of another ransomware, affiliation with the Darkside gang is rumored.

- Haron ransomware debuted in July and is based on Thanos and Abaddon ransomware.
- Doppelpaymar ransomware was rebranded as Grief (PayOrGrief).
- SynAck ransomware was rebranded as El_Cometa in August.

Figure 1. Active Period for ransomware that halted/started operation in 2021

The average life span of the ransomware listed above, that either disappeared or rebranded itself in 2021, is a bit less than two years. Reasons for halting operations vary from one ransomware group to another, but they usually do so to escape the unwanted attentions of law enforcement and security researchers.

Ranion Still Going Four Years Later

The Ranion ransomware variant that FortiGuard Labs recently came across bucks that trend. The Ranison ransomware family appears to have been around since at least early 2017, giving it more than four years of longevity. In February of that year, Daniel Smith at Radware Security shed the first light on the Ranion ransomware, describing it as Ransomware-as-a-service. Surprisingly, its website on the Dark Web has remained relatively unchanged: the Ranion developer still maintains its claim that Ranion was created for educational purposes and asks users not to use the ransomware for illegal activities.

The latest version of Ranion, version 1.21, was released in July 2021. Amazingly, the Ranion developer has updated the ransomware every month in 2021 (except for May), including updates for detection evasion, which casts doubt on the claim that the ransomware is for educational purposes. Another interesting data point is that version 1.08 was released in at least January 2018 and was only updated seven times over a 35-month period (January 2018 – December 2020). However, it has seen rapid acceleration in its development in 2021, with six updates over a seven-month period for unknown reasons. Each update made in 2021 contains additional code using an open-source program named ConfuserEx to evade detection and protect the security vendors' identities. We will touch on this part later.

Ranion RaaS Explained

Figure 2. Top of the Ranion ransomware web page on the dark web

The latest version of Ranion ransomware is designed to encrypt files on a compromised machine using the following 44 file extensions, an increase of five new file types over previous analyses (newly added extensions are highlighted in orange):

.wallet, .txt, .rtf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .ods, .pdf, .jpg, .jpeg, .png, .gif, .bmp, .csv, .sql, .mdb, .db, .accdb, .sln, .php, .jsp, .asp, .aspx, .html, .htm, .xml, .psd, .cs, .java, .cpp, .cc, .cxx, .zip, .rar, .pst, .ost, .eml, .pab, .oab, .msg

Although the ransomware is not designed to encrypt executable files, the Ranion developers state that users "can request other additional file types/extensions to encrypt for free as any files can be a target of Ranion ransomware."

How Ranion Makes Money

Originally, back in 2017, Ranion offered users two support packages (a 1-year and a 6-months service). Today, the Ranion team offers four support packages: Elite, Premium, Standard, and Test.

	Elite	Premium	Standard	Test
32-bit Ranion Ransomware	○	○	○	○
64-bit Ranion Ransomware	○	○	○	○
Decrypter	○	○	○	○
Subscription Duration (month)	12	12	6	1
Reward Percentage	N/A	N/A	N/A	N/A
Ransomware Features				
Delayed Start	○	○	○	○
Delayed Encryption	○	○	○	○
Task Manager	○	○	○	○
Registry Editor Disabler	○	○	○	○
UAC Bypass	○	○	○	○

Desktop Wallpaper Change	○	○	○	○
IP Tracking	○	○	○	○
Offline Encryption	○	○	○	N/A
Support	○	○	○	N/A
Real-Time Client Manager	○	○	○	N/A
Add-On: Dropper (+90 USD)	○	AUP[1]	AUP	N/A
Add-On: Clone (+90 USD)	○	AUP	AUP	N/A
Add-On: FUD+ (+300 USD)	○	AUP	AUP	AUP
Add-On: Unkillable Process (+90 USD)	○	AUP	AUP	N/A
Price (USD)	1900	900	490	120

Figure 3: Ranion ransomware packages and prices

Previously, the most expensive package was offered for 0.95 bitcoin and the cheapest for 0.60 bitcoin. In February 2017, one bitcoin was worth about 1,200 US dollars, which means these packages sold for around 1,140 USD and 720 USD, respectively. As of September 2021, one bitcoin exchanged for around 50,000 USD so Ranion developers have adjusted their prices, and they also now offer discounts for easy-to-buy add-on options.

Ranion's business model is quite different from other RaaS vendors. Typically, Ransomware-as-a-Service vendors pay out 60%-80% of any ransoms collected to their "affiliates" that have successfully installed their ransomware onto a victim's machine. The Ranion developers do not take a middleman's cut. Instead, their affiliates pay for the RaaS service upfront, and they then receive 100% of any ransoms collected. And while some RaaS vendors try to recruit experienced affiliates, and often screen potential affiliates before allowing them to sign up for the service, Ranion developers do not. This is one of the reasons why many inexperienced affiliates start with Ranion. It allows then to get used to the ransom operation. It is also a choice for affiliates who were unable to pass the screening process imposed by other ransomware gangs, thereby lowering the bar for entry.

To see how well this model works, we tracked some Bitcoin wallets used by one of the older Ranion samples for ransom payment. Two moderate payments, totaling about USD $153 and $460 worth of Bitcoin, were made to the wallet within a week of the Ranion sample being made available. But a Bitcoin wallet used by Ranion has recorded transactions from two other Bitcoin wallets. About $4.7 million USD worth of Bitcoin was transferred to one of those wallets from over 300 different Bitcoin wallets.

Dropper Add-On

Another notable characteristic of Ranion is that it provides an opportunity for buyers to purchase a dropper add-on. At first glance, a "dropper" may sound like a malware add-on that Ranion affiliates can use to deliver ransomware, but it's not. According to an FAQ posted on the purchase site, the add-on dropper has the following description: "*RANION can download a program of yours (exe file) and execute it after encryption process ended.*"

For example, an attacker might use this add-on to silently download and install a remote access tool "RAT" on a victim's machine infected with Ranion. Even if the victim opts to pay ransom, the Ranion decrypter only decrypts the encrypted files but does not remove the RAT. The Ranion affiliate can then turn to other RaaS services that are willing to purchase existing corporate access (recent Lockbit 2.0 and Blackmatter RaaS quickly come to mind) and sell that compromised victim for additional profit. This scheme can surely be "educational," but it's only good for ransomware affiliates.

[1] *AUP is available for purchase*

Figure 4: FAQ on paid "Dropper" add-on.

Figure 5: Sample of Ranion's C&C dashboard

The Ranion Ransomware Delivery Method

The Ranion ransomware's delivery method recently observed by FortiGuard Labs is very straightforward. It was done through a spearphishing email with a zip file attachment that included the Ranion ransomware executable. As Ranion is more suited for beginner threat actors, the lack of sophistication in their ransomware delivery might be a reason why Ranion has not gained household status in the ransomware realm. This may also be why they have managed to stay under the radar for more than four years.

Figure 6: Recent spearphishing emails (in Spanish and French) used to deliver the Ranion ransomware

Ranion's ransom message supports eight languages by default (English, Russian, German, French, Spanish, Italian, Dutch, and Persian). Any regions in which those languages are primarily used can be a target of Ranion.

Ranion Ransomware Origin: HiddenTear Copycat?

Ranion bases its code on the open-source proof-of-concept ransomware known as HiddenTear. There are some code similarities between the two projects.

Figure 7: HiddenTear AES encryption

The above screenshot is from HiddenTear's implantation of an encryption function. It can be found at https://github.com/goliate/hidden-tear/blob/master/hidden-tear/hidden-tear/Form1.cs. For comparison, Ranion's implementation is below:

Figure 8: Ranion AES encryption

To encrypt files, HiddenTear uses this function.

Figure 9: HiddenTear file encryption

Ranion implements its encryption in a similar fashion.

Figure 10: Ranion file encryption

These are just two examples. Overall programming resemblance can be seen in a variety places. In addition, Ranion kept their resource section similar to HiddenTear's as well.

Figure 11: Ranion resource

NOTE: This Ranion variant is from 2017 and has a SHA256 hash value of eed03a9564aee24a68b2cade89d7fbe9929e95751a9fde4539c7896fda6bdcb5

To Be FFFFUUUUDDDD

To be fully undetectable, the Ranion team has consistently relied on the ConfuserEx project, which is the successor of the now defunct Confuser project. It is a free and open-source obfuscator that makes malware harder to analyze by "protecting" .NET applications through symbol renaming, anti-debugging, encryption, compression, and other functions. (For more info, please see the github project page here.)

The 2017 Ranion variant analyzed below was "protected" by the Confuser project.

Figure 12: 2017 Ranion using Confuser

The following 2021 variant of Ranion was "protected" using the ConfuserEx project.

Figure 13: 2021 Ranion using ConfuserEx

While ConfuserEx is able to do what it says, which is "protect" .NET applications, in this case it is protecting malware from being detected by the AV industry via evasion techniques.

Conclusion - Ranion Ransomware

HiddenTear-based Ranion is a low-profile, low-cost RaaS that has not achieved the same success of other, more notorious ransomware gangs. However, this ransom service provides enough basic features for new threat actors to use it as a steppingstone for working with more sophisticated malicious services. Ranion is only “educational” in that it helps train wannabe cyber criminals inflict the same damage as other ransomware variants that have simply adopted more polished and sophisticated delivery and propagation mechanisms.

Fortinet Protections

Fortinet customers are already protected from this malware by FortiGuard’s AntiVirus and FortiEDR services, as follows:

MSIL/Kryptik.LMX!tr

MSIL/Agent.AZG!tr

MSIL/Agent.BJU!tr

MSIL/Bladabindi.FM!tr

MSIL/Filecoder.FU!tr

MSIL/GenKryptik.BLYY!tr

MSIL/GenKryptik.FEWS!tr

W32/Crypmodadv.A!tr

W32/DOTHETUK.FU!tr.ransom

W32/Hesv.BXFI!tr

Indicators of Compromise (IOCs):

SHA2:

52f6e8c0c28f802d8dfd9138bcc971d449d0526469a36541359b6fc31d44d7dc

d63f032180d6cbc3165f79dac13f81e69f3176b06f0ff4b162b167e4f45f5e93

f687c51ee4889c6a35536d06c87b0123d17a483f7e2f5efcfb423fba94e186be

f18044a85ceb3c472ae57e3473e2f14f945f22a9df634caa242b11e5f81c561b

e4c42969a0327ce133b8b6dd52b0f2e926fbc43a48cf2abbd78d521e310b00e4

41ad23008aea13bccf60249c24ee290e9867223d783bc9ddc4234b8e1d21008d

d894cfa1f2e55ea8fb61598d1312d92c6c1667f97ec683dfa5b5350b32402099

2a8f7abaa6b896bdcc8f73a78af89274df5ee5f586edb88a0b4fd0b06cbaf6bd

19b2da9261d163d3a8e25916b0c960bae36d4334172faa2eb7f720c7483f0fb1

434bbb0e4f289944e6c1fafc11e7f3353056857fb90abafd17e2c6ec697d94b3

bbe77c293bf11c5e8d26ff1583cf546a346de5d666e5558b17f056f1117ddaf8

7afbb979ac6485cbe4d21955dd0f4444d67d2b99aa3d420c09bcc7d54949ed7c

ac5e6f8e646311bf3645ccdccf7119712ada6811d973444d3a763d17083ef028

2ab7ba4aa579ffda113b3f1a693cb2f6b45c5adb833301762d623089f5e37694

4ad4aabd3ec941e6eb442aadae23e01539f63c093582ebf9239681fe399c7571

e28afea1a286b27c9f4578cb27729e180dd20f406282e489328e11722b37af73

8a4298a5c2101baf0315a2c5ed297a6b9912c673a200a7082fb96fcaa21a7316

798a618bf3b817751de722bc84475d5dca798fb48e844804d530e34e920fad09

bd82bb30089383547fcc1ab8181c957f770a99c1499db211fa3245135fcce2be

eba37b0cef846c16bca30804557d7dae57b16cda506a111e2e4c6f7ef54cab70

507cc65037febbad93cd5a4c10d1e870f4f73069484bd7913349deb139c18ea2

b93a45691e955d4600dde6219125f0a38b0544ad48872bc4ebda5436cf2c0bc0

abf13688180d505d07b04a6643941a571de1efd97b46631abfafd555863ec33e

0f2bbf749501297928efbd4a12d8a1858c7944516e8b15817988a429eae4e632

a9671f6455895b1e0875eec277015672ea816dc5299cfd519db2dc4bc38ce693

0a59c6b2ec5dbaa7e36b52dc494d1e58e918f32695cfb28104a5c82b09a9554f

ca7aaa3de1948dc882d55d40a0269a145e34f1e07b2b1e932040863e6d1dedb8

27cb1df4a3092c42ddfd93db50cc78813a823a881e6d131410915d0ded6515c4

46b9c46520f00b25924cc0a137393f67a0f4395da8cdc37b32985b90d7285252

46462ba2ac8018901239800f1c4562a31618b1565fe559ab826feef303adab8d df7c5267c9e61d7b23a3a771623c6b274fb601023725a8af1b8bc25ae8bcbdb6

0085d31140895d16a2f92a77b62fb50db0d05fa47b447e21bca062532b5bf0d2

780a576b7ea69b46eb8a698aac0c6ee6e2e426fddcd7a99b749f5aa083e8f72b

94968c73dacfd68500ca59905e410ca4ccafe92cd8e223ed47ad916ee82a6dfb

c18c9cf30056d9ebfda69bb9869a38b5ab2d2e3d388a747d7ec8516e022aa7e9

19d9ec2713d913d5325a72ce646351a2384d86efd5dcecebb354ef2bc9e801a2

c38e068677903ccd9b117bacaa3b201616668e449856f8d14894f9acf3f6e9cc

378b34a3e1f760dc7d6c5ff742c543a0184a255c7c3422e348eab05dca1377f9

e9352eb25a1ef3fc8d88fd62a4253d4b8db3931366f012e9ee7916818f74ad55

f7b6ac95cbf4f4122c67e3f841de1152cb032e36d768cd71618cbaf95f131727

df16d6b57a0290b8d7276285020cf6cf5e7c4a561516500fd44e862ea32c1073

dbd00dffb77998d4b0c9946e727279831f19e5d58059b0de353cb191f6c3ca00

1bbc33db0c52d5c3f2798f726bb476cf20d00eeae971e98926bbfbf194e7e03c

98f16b75d1c9e3c8914b10de4b6286397285d226785b42766847b35558ee0dc7

86c6a8c1cd461dafdc30ce37eca355f096ff35ccd48b4de3f2f3bd56d0cef543

c5234f098cf2319c813e8025e0ea04b4f45de4ad195b64ba80fe9a098de54431

0361585476c9e04cbe9efac74fe76e32d84e2e682ac4a8e5f67860a719e7b6d0

1fdaae6a5b1d69d795a07b5518568964dc53e181b22ad2427e7f10c60d61241b

4824c68f18089c44af8426b9a2d7960f5caa572777a46b3a172093b321acbf1d

eed03a9564aee24a68b2cade89d7fbe9929e95751a9fde4539c7896fda6bdcb5

023b12665ff5c46331ece74d220c52a28439ada61210183bbd921e1ef833645c

aa9bbffae11e2a2af53acbb56129d99cb93c78c98202f5c19b095f9ed296a2ce

ea00fffa874669e743d125fcdb55ba591a54d469c621eada61f304495269a35c

f389a83b1309ff17c9c0faf1d9e079ceae3b4111c6813ad50bd451a9a19b291b

33d24a576f00847d44315c1d6d588a3aa45031dec2b1590bc67bc6800e455cf6

MITRE ATT&CK information

Execution

- T1204.002: Malicious File

Persistence

- T1547.001: Registry Run Keys/Startup Folder

Privilege Escalation

- T1548.002: Bypass User Account Control

Defense Evasion

- T1027.002: Software Packing

- T1548.002: Bypass User Account Control

- T1562.001: Disable or Modify Tools

Discovery

- T1083: File and Directory Discovery

Impact

- T1486: Data Encrypted for Impact

- T1491.001: Internal Defacement

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.

Learn more about Fortinet's free cybersecurity training, an initiative of Fortinet's Training Advancement Agenda (TAA), or about the Fortinet Network Security Expert program, Security Academy program, and Veterans program. Learn more about FortiGuard Labs global threat intelligence and research and the FortiGuard Security Subscriptions and Services portfolio.

Related Posts