Ransoms Without Ransomware, Data Corruption and Other New Tactics in Cyber Extortion

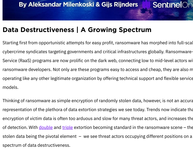
October 20, 2022
By Aleksandar Milenkoski & Gijs Rijnders (Cyber Threat Intelligence - Netherlands Police)

PDF

Much like legitimate businesses, ransomware operators adjust their operational strategies to achieve results while managing time and resources, and defenders are required to track these shifting strategies to maintain effective protection. Presently, we are observing an evolution in how cyber criminals approach the business of extorting money from organizations.

Ransomware actors have turned toward data theft instead of time-expensive encryption, and importantly, the anatomy of modern extortion attacks involves operators taking different approaches to data destruction from full encryption to partial encryption to no encryption – and, thus, no ransomware – at all. What the cybersecurity industry generally refers to as 'ransomware operators' must now be thought of as a subset of a larger group of threat actors who occupy different positions on this spectrum of data destructiveness.

In this post, we describe this emerging spectrum of data-focused threat actors to help defenders better understand the continuing development of data extortion tactics, techniques, and procedures (TTPs).



Data Destructiveness | A Growing Spectrum

Starting first from opportunistic attempts for easy profit, ransomware has morphed into full-scale cybercrime syndicates targeting governments and critical infrastructures globally. Ransomware-as-a-Service (RaaS) programs are now prolific on the dark web, connecting low to mid-level actors with ransomware developers. Not only are these programs easy to access and cheap, they are also mature, operating like any other legitimate organization by offering technical support and flexible service models.

Thinking of ransomware as simple encryption of randomly stolen data, however, is not an accurate representation of the plethora of data extortion strategies we see today. Trends now indicate that full encryption of victim data is often too arduous and slow for many threat actors, and increases the risk of detection. With double and triple extortion becoming standard in the ransomware scene – the stolen data being the pivotal element – we see threat actors occupying different positions on a spectrum of data destructiveness.

At one end of the spectrum are threat actors that do not destroy data at all and therefore spend no time on this activity – they only steal data that is valuable to victims as a means to extort them. At the other end of this spectrum are actors that use traditional ransomware to cause business loss, either encryption to destroy data completely. The rest of the spectrum is populated by actors that steal data and either partially or fully destroy it to damage their victim's infrastructure, thus gaining additional leverage over them.

The data destructiveness spectrum

Ransoms Without Ransomware

This strategy is exemplified by two relatively recent threat groups, Karakurt and Lapsus$. Both leverage data extortion-only methods in their campaigns. Neither group deploys ransomware on compromised systems. Instead, they exfiltrate data and use the stolen data as leverage, joining the ranks of groups such as Markets and BlackTOR.

The Twitter profile @MamounGatt introducing Markets (source: Digital Shadows)

Karakurt typically gains access to networks through initial access brokers (IABs) or by exploiting vulnerabilities in internet-exposed network services such as outdated Fortinet FortiGate SSL VPN appliances. The threat group is considered to be the data extortion arm of the now defunct Conti syndicate. Karakurt has targeted victim across all industries and geographical regions.

Karakurt sends victim-specific emails to employees revealing that data has been stolen while threatening that the data will be leaked to competitors or auctioned online. The extortion note contains employee names and indicates that Karakurt has spent a considerable amount of time locating data that is valuable to the victim organization to ensure the group's extortion leverage.

```
[...]
Hi,
We are also reading this - so it means that we have your attention.
Here's the deal:
1. We downloaded your internal network and took control over all of your systems.
2. We analyzed and located each piece of more or less important files across spending weeks inside.
3. We prepared everything so better (the total size of taken data needs 500 GB).

FAQ:
- Why the hell are you guys?
- Money motivated hackers I guess.
- Why should I care?
- Well, we are not a charity.
- Why should I care?
- We are going to report this to law enforcement.
- This activity can lead to huge fine and/or penalties most of your IT infrastructure, and even if
  you're not directly responsible, you will lose your job. - Why will we do that?
- Why else already knows about the breach?
- Mm, Tesla, Cisco Systems, Fox News, Nissan Motors, Steven Madeiros, Sergio Tomas,
  Sergio Domiciliro, Sylvia Pedro, Margarita Domiciliro, Irina Tomas, Valtina Mobile, Angel Holiday,
  Sergio Domiciliro, Sylvia Pedro, Margarita Domiciliro, Irina Tomas, Valtina Mobile, Angel Holiday,
  Sergio Domiciliro, Sylvia Pedro, Margarita Domiciliro, Irina Tomas, Valtina Mobile, Angel Holiday,
  [...]
- What if I told you that I do not care and going to ignore this attacks?
  That's a very bad choice, if you will not contact us in a timely manner (by 20 October 2021) we will
  start sending your sensitive information to partners, competitors and any other persons that should know how you
  treat your corporate secrets and thefts.
[...]
- What if I will not contact you ever after 20?
  Well, we will start sending your sensitive data to growing your business competitors and list of anonymous inside
  traders on dark web, so that all of they are going to pay or the risk of being sued. When the risk of being sued is
  increased to such data is formed - the issue becomes active chaotic.
[...]
- Why should I care? - Well, we are reasonable.
  We know business well - we will give you reasonable offer, making sure that this leak goes straight to
  the grave. We will make sure that your business will bloom by using any power we have in our possession, both social and technical.
[...]
```

Karakurt extortion note (trimmed for brevity)

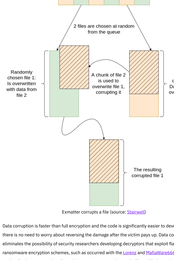
In contrast to Karakurt, Lapsus$ uses stolen credentials and phishing to gain initial access to networks. The group then uses SIM-swapping, social engineering, and solicitation methods to bypass multi-factor authentication (MFA).

Lapsus$ has recently targeted victims in the high-tech industry, notably Nvidia, Samsung, Okta, Microsoft, and Ubisoft. The threat group is also known to attack organizations specifically to gain access to their customers. Such has been the case with the Okta breach in early 2022. It is interesting to note that Lapsus$ conducts data extortion campaigns not only for financial gains, but also to increase their notoriety.

Extortion Through Data Corruption

Some ransomware operators are now implementing data destruction techniques that are more lightweight and time-efficient than data encryption. Through data corruption, operators are capable of driving urgency in their victims as well as escalating their ransom request.

Exemplifying this is the new version of the Eternalter data exfiltration tool which corrupts data by replacing a data chunk of a file with a data chunk from another file. This change in the implementation of Eternalter strongly suggests the beginning of a new trend in ransomware operations where threat actors seek to corrupt data instead of encrypting it.



Eternalter corrupts a file (source: Sophos)

Data corruption is faster than full encryption and the code is significantly easier to develop, since there is no need to worry about reversing the damage after the victim pays up. Data corruption further eliminates the possibility of security researchers developing decryptors that exploit flaws in ransomware encryption schemes, such as occurred with the Locky and MyBadBreaks ransomware strains. In short, corruption allows threat actors to save time and effort while improving their chances of a successful payout.

The Growing Trend of Partial Encryption

An increasing number of ransomware operations have joined the trend of partial or intermittent encryption that the LockFile ransomware started in mid-2021. A previous SentinelLabs article reviewed recent ransomware families that conduct intermittent encryption, such as BlackCat, BlackBasta, Agenda, and Quiva.

Royal ransomware is a new member of the ransomware scene which employs partial file encryption methods. This ransomware skips the encryption of file content blocks 10 times – the total number of the encrypted bytes between the blocks which amounts to the percentage that the ransomware operator has configured through the op command-line parameter.

```
50 c2 08 27 fa b2 d8 ff 20 f5 52 c1 20 7f 74 7a   .L.Lime-conte...
bf 05 ff c4 ab 28 f5 b4 ed f7 81 cf 8f 84 f8 f8   ?Ar*Ki?Ki-ri-r
83 17 24 b1 97 5b 89 4c 40 b6 ff 70 40 7c 8b 1f   *?X?Ki?Ki-ri-r*
ff 5a 8b 1f 40 7c 8b 1f 40 7c 8b 1f 40 7c 8b 1f   ?Ki?Ki-ri-r?Ki
24 b1 a8 c9 50 7c 5c 82 5b 1c 20 f5 f5 5b 20 f5   Back up!-or-Ba
8f 7b 52 b9 20 c2 7c 7c 8f 20 a6 b9 7c 12 c7      ck Back up!-or-
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

The new Royal ransomware conducts intermittent encryption (the null bytes represent non-encrypted file content)

Partial encryption allows ransomware actors to destroy data faster than with full encryption. The gains in time are especially noticeable when it comes to encrypting large files, where the time spent on encryption per file is reduced in the order of minutes.

Partial encryption may also help threat actors to evade security mechanisms that detect ransomware by monitoring the intensity of file IO operations or by evaluating the entropy between non-encrypted and encrypted versions of a given file, for example, based on Chi-squared or data entropy measures.

What's Next for Data Extortion?

Changes in the threat landscape have created differing trends in how data is leveraged to increase the chance of successful ransom. We predict that data extortion actors, including ransomware operators, will continue to occupy different positions on the data destructiveness spectrum.

Ransomware actors that steal data to extort their victims also aim to gain additional leverage by damaging the targeted infrastructure, disrupting business services and causing both reputational harm and financial loss. This type of actor will likely continue to resort to a combination of data destruction techniques, corrupting or partially encrypting large files where speed is of the essence, but continuing to fully encrypt others. Some actors may focus more on corruption to avoid potential implementation flaws in encryption schemes.

Meanwhile, extortion actors that seek to use the value of stolen data without conducting any encryption at all are set to gain further momentum within the threat landscape.

We also anticipate the emergence of a hybrid model amongst threat actors that will allow them to switch between conducting data theft only and using a more traditional data-destructive ransomware approach. At the core of this model is the value of the stolen data. Depending on its value, threat actors will evaluate whether or not it is sufficient as the only means of extortion leverage.

Conclusion

The profitability of the ransomware industry has given way to a multitude of extortion methods. What's emerged is a spectrum of threat actors who are moving past traditional, time-consuming encryption focused on destroying all stolen data. Now, actors are seen prioritizing faster attacks either through data extortion, where the data is more or less preserved, or only partial corruption allowing them to move quickly and demand increasingly larger ransom demands.

This spectrum of attack methods is the result of a gradual process, influenced by the development of decryption and other malware-detection capabilities as well as the professionalization of malicious actors themselves. As demonstrated by the trends outlined in this post, actors have clear ambitions and continue to adjust their methodologies and tactics to capitalize on the most likely targets and payouts.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- OpenSSL 3 Critical Vulnerability | What Do Organizations Need to Know?
- SmoothOperator | Ongoing Campaign Trojanizes 3CXDesktopApp in Supply Chain Attack
- PrincessOtha's Snapchat Executive Brief | Swarm Geopolitics and Network Warfare
- Gaoxon Brings Cobalt Strike Capabilities to macOS Threat Actors
- Enterprise Security Essentials | Top 12 Most Routinely Exploited Vulnerabilities
- BlueNoroff | How APT38's macOS Rootkitchen Seeks to Evade Analysis and Detection