Ransomware and Data Leak Site Publication Time Analysis

vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/

Corsin Camichel April 25, 2021

Ransomware – the threat that breaches a victim network, steals data, encrypts local systems and published the stolen data
– (image by mohamed_hassan)

Ransomware

What was once a threat to every internet user due to the wide-spread nature of campaigns – infect as many devices as possible, extort for a small ransom – has turned into a multi-million dollar payment game. Ransomware operators are now playing in the big league. Ransom demands in the $50M range have now been seen several times, payments in the tens of millions are not unheard of.

For the past year I have been monitoring ransomware and data leak sites. What initially started as a website refresh several times a day has turned into a fully automated system that tracks 20+ leak sites, browses all listing pages, extracts victim name, publication date and some other details, parses the output, compares it to the last run and notifies subscribers of the newly listed victim.

An interesting output of this project is the fact that the sites are monitored 24 hours a day, 7 days a week. This allows me gain to interesting insight when ransomware operators are working by publishing victim data. Yes, I believe some data leak systems are automated and no human is pushing a button, but for some leak sites you can identify patterns of working hours.

For the below analysis I reviewed the data between December 2020 and April 2021 from leak sites with more than 35 new victims listed. the following nine ransomware and leak sites made it into the analysis:

Name	Victim Count
Avaddon	107
BABUK	51
CL0P	42
Conti	192
DarkSide	126
DoppelPaymer	71
Nefilim	36
PYSA	135
REvil	107
Total	867

Table: Ransomware and data leak site victims (December 2020 to April, 2021)
The first interesting observation that stands out, is that **PYSA** has four slots, in which they publish their victims. The vast number of victims are listed in the hour starting at 00:00 UTC and 11:00 UTC. Only a handful of victims are added after 06:00 UTC and after 15:00 UTC. I can say with high confidence that this is likely the result of automation on their end. This is also supported by the observation that PYSA leaks many victims at the same time, in one go.

Almost the opposite can be seen by looking at the publication times of **Conti**. The operators behind this leak site spread publication across the full day, with increased publications in the hours of 08:00 UTC, 09:00 UTC and 22:00 UTC.

For some other leak sites you can see some down-time, off-work hours. In my opinion, **CL0P** is a great example of this behaviour. No new victims were listed between 01:00 and 10:00 UTC, the night time in Europe and neighbouring countries.

Enough pre-text, here is the output table:

Name	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Avaddon	9	5	15	14	2							17		4	8	10	4	2	4	4	2		2	5
BABUK		5							1	2	3	10	2	3	2	9	2	6		1	3			2
CL0P	1										3	4	5	6	11	5	2	2			1	1	1	
Conti	3	6	1	5		2	1	2	16	21	8	8	4	12	12	14	7	5	7	10	2	11	30	5
Darkside	2		2		2	2	2	3	1	3	3	4	5	3	12	8	8	43	3	4	3	4	5	4
DoppelPaymer			1			9	1	7		3		3	1	8	8	15	7	2	1	3		1	1	
Nefilim				1				2	3	3	1	1	3	2	1	1	2	1	1	1	2	4	6	1
PYSA	50						8					69				8								
REvil	1			2	1	1	4	16	3	7	7	11	3	5	3	7	10	3	9	2	6	1	2	3

Table showing publication hours of data leak sites (initial victim posting hour only)

The list above contains publications on any given day of a week. If you want to look at the data only for working days, see the screenshot below:

Name	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Avaddon	9	4	10	10	1							17		1	5	8	2	2	3	3	1		1	5
BABUK		4							1	2	1	9	1	3	2	6	2	5		1	2			2
CL0P	1										3	4	5	6	11	5	2	2			1	1	1	
Conti	3	6	1	2		2	1	1	16	21	7	8	4	12	12	13	7	5	7	9	2	9	27	5
Darkside	1		1		2	2	1	2	1	3	2	3	5	2	12	4	7	43	3	4	2	2	5	2
DoppelPaymer			1			9	1	7		3		3	1	8	8	15	7	2	1	3		1	1	
Nefilim				1					3	2		1	3	2		1	2		1	1	2	3	5	1
PYSA	50						8					69				8								
REvil	1			1	1	1	4	5	1	6	7	11	2	4	3	6	8	2	8	1	6	1	1	3

Table showing publication hours of data leak sites (Monday – Friday)

And for publications only on a weekend, this is it. You can see that three groups (**CL0P**, **DoppelPaymer** and **PYSA**) do not publish victims on a weekend, as they are missing in the table.

Name	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Avaddon		1	5	4	1									3	3	2	2		1	1	1		1	
BABUK		1									2	1	1			3		1			1			
Conti				3				1			1					1				1		2	3	
Darkside	1		1				1	1			1	1		1		4	1				1	2		2
Nefilim								2		1	1				1			1				1	1	
REvil				1				11	2	1			1	1		1	2	1	1	1			1	

Table showing publication hours of data leak sites (Saturday and Sunday)

What are your take-aways? Agreeing or disagreeing with my assessment? Do see a different pattern that you want to discuss? Let me know, I am very interested in seeing your views on this.