



# Gone in 52 Seconds...and 42 Minutes: A Comparative Analysis of Ransomware Encryption Speed

By [Shannon Davis](#) March 23, 2022

**D**o you feel like every other cybersecurity news story mentioned ransomware in 2021? Does it feel like you can't turn on a cybersecurity podcast and not hear the "R" word? We feel the same way, and as a cybersecurity vendor, we felt that we should also contribute to the noise. :-)

But we did want to try and do something different. On top of Splunk's numerous [ransomware detections](#) from our threat research team, we wanted to use Splunk to see if we could add some refinement and knowledge to the ransomware clamor. We decided to measure how fast ransomware encrypts files; not just one or two ransomware binaries, but dozens of them — all using Splunk.

Why? Well, partly because we have an unlimited Splunk license, but also because we couldn't find the answer to the question: "How long do you have until ransomware encrypts your systems?" This seems like knowledge that organizations could use to organize their defenses. If organizations have more than 20 hours before ransomware finishes encrypting, they might choose to focus on detecting and mitigating ransomware after infection. If ransomware encrypts an entire system in 52 seconds, organizations should probably respond earlier in the ransomware lifecycle. In our initial hypothesis, we asserted that if ransomware executes on a system, then it's too late for an organization to respond effectively. We conducted a literature review of ransomware encryption speed and only uncovered work that was encyclopedic in scope from one of the ransomware groups themselves.

The LockBit group posted a table on their Tor site (Fig. 1) listing encryption speeds for more than 30 ransomware families, showing — perhaps not surprisingly — that LockBit was the fastest. To be fair, I guess that makes sense; you typically don't release PR pieces that highlight how bad you are. We then looked at dwell time for ransomware intrusions and found that the three-day dwell time cited by Mandiant in their [2021 M-Trends report](#) was fairly representative. This gave us a “how long till people realize they are infected with ransomware” timeframe.

<i>Encryption speed comparative table for some ransomware</i>							
PC for testing: Windows Server 2016 x64   8 core Xeon E5-2680@2.40GHz   16 GB RAM   SSD							
Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
<b>LOCKBIT 2.0</b>	<b>5 Jun, 2021</b>	<b>373 MB/s</b>	<b>4M 28S</b>	<b>7H 26M 40S</b>	<b>Yes</b>	855	109964
<b>LOCKBIT</b>	<b>14 Feb, 2021</b>	<b>266 MB/s</b>	<b>6M 16S</b>	<b>10H 26M 40S</b>	<b>Yes</b>	146	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130	110468
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115	111002
RansomEXX	14 Dec, 2020	138 MB/s	12M	20H	No	156	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364	random extension
Sun Crypt	26 Jan, 2021	104 MB/s	16M	1D 2H 40M	No	1422	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186	110220
Ryuk	21 Mar, 2021	92 MB/s	18M	1D 6H	Yes	274	110784
Zeppelin	8 Mar, 2021	92 MB/s	18M	1D 6H	No	813	109963
DarkSide	1 May, 2021	83 MB/s	20M	1D 9H 20M	No	30	100549
DarkSide	16 Jan, 2021	79 MB/s	21M	1D 11H	No	59	100171
Nephilim	31 Aug, 2020	75 MB/s	22M	1D 12H 40M	No	3061	110404
DearCry	13 Mar, 2021	64 MB/s	26M	1D 19H 20M	No	1292	104547
MountLocker	20 Nov, 2020	64 MB/s	26M	1D 19H 20M	Yes	200	110367
Nemty	3 Mar, 2021	57 MB/s	29M	2D 0H 20M	No	124	110012
MedusaLocker	24 Apr, 2020	53 MB/s	31M	2D 3H 40M	Yes	661	109615
Phoenix	29 Mar, 2021	52 MB/s	32M	2D 5H 20M	No	1930	110026
Hades	29 Mar, 2021	47 MB/s	35M	2D 10H 20M	No	1909	110026
DarkSide	18 Dec, 2020	45 MB/s	37M	2D 13H 40M	No	17	114741
Babuk	4 Jan, 2021	45 MB/s	37M	2D 13H 40M	Yes	31	110760
REvil	7 Apr, 2021	37 MB/s	45M	3D 3H	No	121	109790
BlackKingdom	23 Mar, 2021	32 MB/s	52M	3D 14H 40M	No	12460	random extension

Figure 1. LockBit analysis of ransomware encryption speeds among competing ransomware groups.

# Prep Work

We couldn't leave it to LockBit's marketing team to only release content like this, so we rolled up our sleeves and got busy building an environment that would allow us to conduct our own ransomware speed tests. We took the great [Splunk Attack Range](#) project, created by [Splunk's Threat Research Team](#), and modified it to fit our needs.

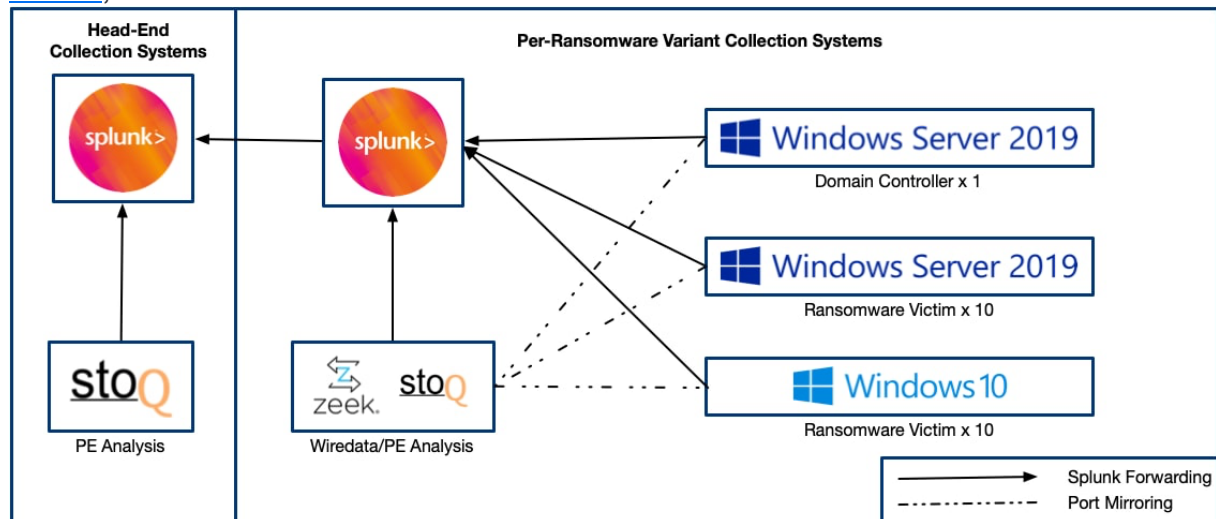


Figure 2. Diagram outlining the ransomware environment created using a modified version of Splunk Attack Range.

We created four different “victim” profiles consisting of Windows 10 and Windows Server 2019 operating systems, each with two different performance specifications benchmarked from customer environments. We then chose 10 different ransomware families and 10 samples from each of those families to test. Figure 3 outlines the families that we tested, along with the Microsoft Defender detection identifiers from VirusTotal.

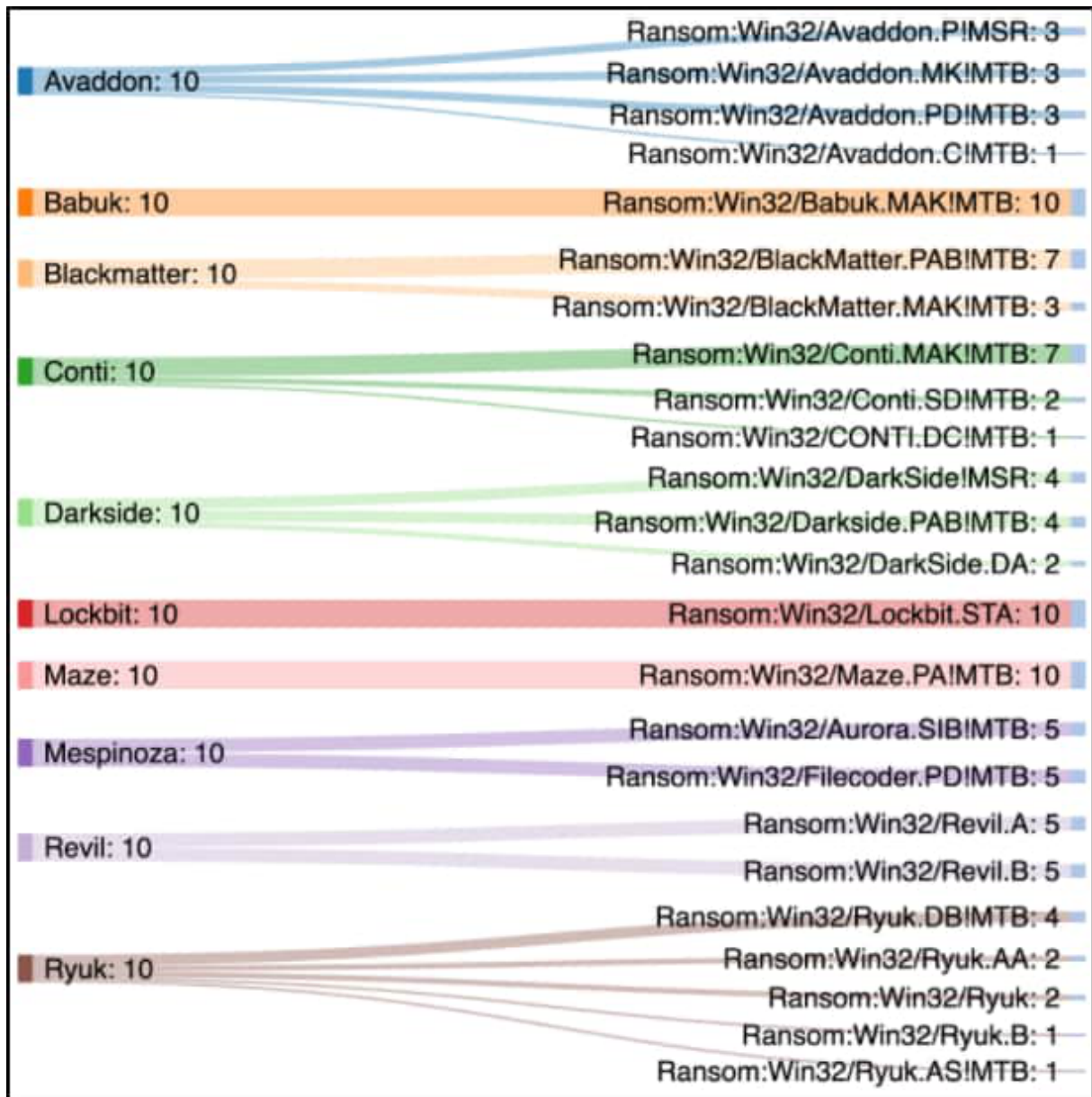


Figure 3. Ransomware families and corresponding Microsoft Defender detection identifiers from VirusTotal.

We tested every sample across all four host profiles, which amounted to 400 different ransomware runs (10 families x 10 samples per family x 4 profiles). In order to measure the encryption speed, we gathered 98,561 test files (pdf, doc, xls, etc.) from a public file corpus, totaling 53GB. To collect the necessary data, we used a combination of native Windows logging, Windows Perfmon statistics, Microsoft [Sysmon](#), along with [Zeek](#) and [stoQ](#) for further analysis (that's content for future blogs, so be patient).

In order to capture the required encryption events, we enabled [Object Level Auditing](#) on the 100 directories where our test files lived. This provided us with [EventCode 4663](#) logs that we could use to calculate the Total Time to

Encryption (TTE) for each sample. The samples we tested had an Accesses value of DELETE at the end of encrypting each file, which is how we measured encryption speed. Not all ransomware behaves this way, so a search for EventCode=4663 Accesses=DELETE in Splunk may not always return the same results.

## The Heist

Just like watching *Gone in 60 Seconds* (the Nicholas Cage version, of course), you're on the edge of your seat waiting for the results. Well, here you go.

Family	Median Duration
LockBit	00:05:50
Babuk	00:06:34
Avaddon	00:13:15
Ryuk	00:14:30
Revil	00:24:16
BlackMatter	00:43:03
Darkside	00:44:52
Conti	00:59:34
Maze	01:54:33
Mespinoza (PYSA)	01:54:54
<b>Average of the median</b>	<b>00:42:52</b>

Figure 4. Median ransomware speed measured across 10 ransomware families.

As you can see, LockBit lived up to its own hype and was the quickest to encrypt of all the ransomware families we tested. We listed the median duration, as some families had one or two samples that would skew the average duration. For example, LockBit had the fastest sample coming in at four minutes and nine seconds (fig. 5). Babuk was a close second but had one sample that was the slowest of all samples tested, which took more than three and a half hours (fig. 6).

Variant	Endpoint	process_name	Duration	Encryptions_Per_Second
Lockbit	Server-2019-High	C:\ransom\lockbit-9.exe	00:04:09	396

Figure 5. LockBit had the fastest ransomware sample to encrypt files with a duration of four minutes and nine seconds.

Variant	Endpoint	process_name	Duration	Encryptions_Per_Second
Babuk	Win-10-Mid	C:\ransom\babuk-5.exe	03:35:08	8

*Figure 6. Babuk had the second fastest median encryption speed but the slowest individual sample, which took more than three and a half hours to encrypt the files.*

## The Getaway

This research is available in a [comprehensive whitepaper](#) with more details than what is outlined here (I get in big trouble for going over 800-1,200 words). As I mentioned earlier, there is more research to come out of our data set. We plan to publish the data to the [Splunk BOTS Portal](#) in time for [.conf22](#) (June 14-17, 2022). This way, you can investigate the data yourself and possibly uncover details that we may not have noticed during our tests.

Finally, you might ask what this means if you're a network defender. Well, if we go back to our original hypothesis of ransomware being too fast to defend against once it executes on the victim system, that should give you a hint. Start looking "left of boom," where boom is the malware detonation, and assess your capabilities to prevent or detect the ransomware group's behavior. Multi-factor authentication, network segmentation, patching, and centralized logging (couldn't help myself there) are all very good strategies to bolster your defenses against ransomware or any other malicious actors for that matter (I'm looking at you, Nicholas Cage). And of course, this sort of work is what you can expect from SURGe over the next couple of months and well into the summer. I mean, someone has to talk about ransomware, right?

Happy Hunting!