Ransomware: Analyzing the data from 2020

digitalshadows.com/blog-and-research/ransomware-analyzing-the-data-from-2020/

January 26, 2021

Note: This blog is a roundup of our quarterly ransomware series. You can also see our Q2 Ransomware Trends, Q3 Ransomware Trends blogs or get our free weekly threat intelligence writeup delivered to your inbox here.

During the final months of 2020, ransomware groups continued to wreak havoc. New variants continued to create data leak sites with the addition of Pay2Key, RansomEXX, and Everest ransomware data leak sites. Ransomware groups continue to target and successfully breach high profile organizations: — Barnes & Noble Booksellers, Inc., Ubisoft, and Epicor Software targeted by Egregor group; Capcom Network targeted by Ragnar Locker group. And, unfortunately, the list of victims continues. If you're looking for the latest details on ransomware in 2020 and the ransomware threat landscape for 2021, read on.

What happened in ransomware for Q4 2020?

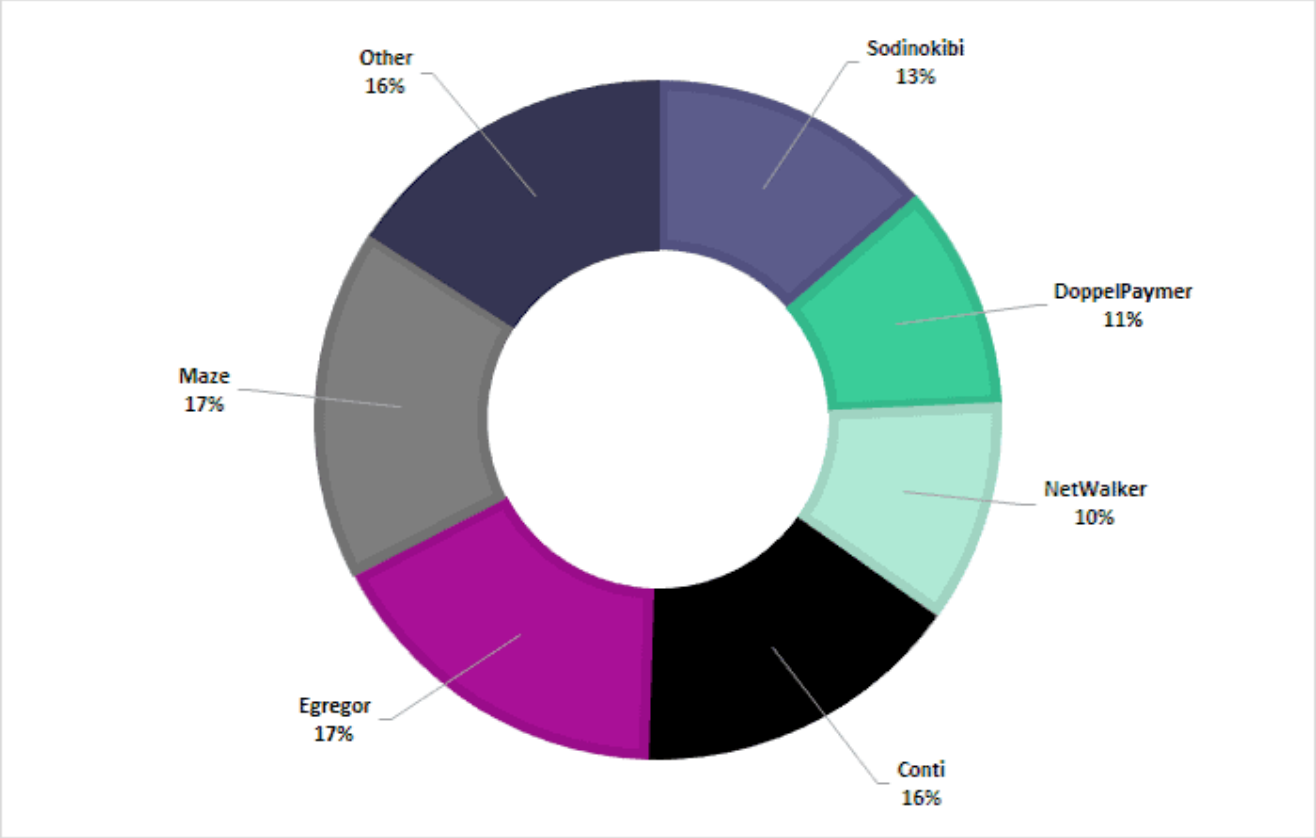
Throughout 2020, we saw the "pay or get breached" trend take off like a rocket and it didn't seem to slow down. To add to the already stressful situation of having their files exfiltrated and encrypted, victim organizations were pressured into paying ransom payments quickly by the threat of public exposure on a data leak site.

In Q4 2020, we identified three additional data leak sites, which is less than Q3 2020 but indicates that this tactic is still viewed as effective and groups continued to use the method. Here's what we identified in Q4 2020:

- In Q3 2020, Maze, Conti, Sodinokibi, and NetWalker made up 76% of our alerts related to ransomware dump sites.
- Ransomware operator activity shifted in Q4 2020, Sodinokibi activity decreased and Maze announced they were ceasing operations. Egregor, Conti, NetWalker, and DoppelPaymer accounted for 71% of our alerts in Q4 2020.
- Pay2Key, RansomEXX, and Everest ransomware groups joined the plethora of data leak sites with their own versions.
- As Maze group announced they were ceasing operations, Egregor entered the scene hitting the ground running with the highest number of alerts for the quarter.
- Ransomware groups attempted new tactics, which included cold calling victims to pressure them into paying the ransom demand; some attempts went as far as threatening employee's safety.

Who was the most active ransomware group of 2020?

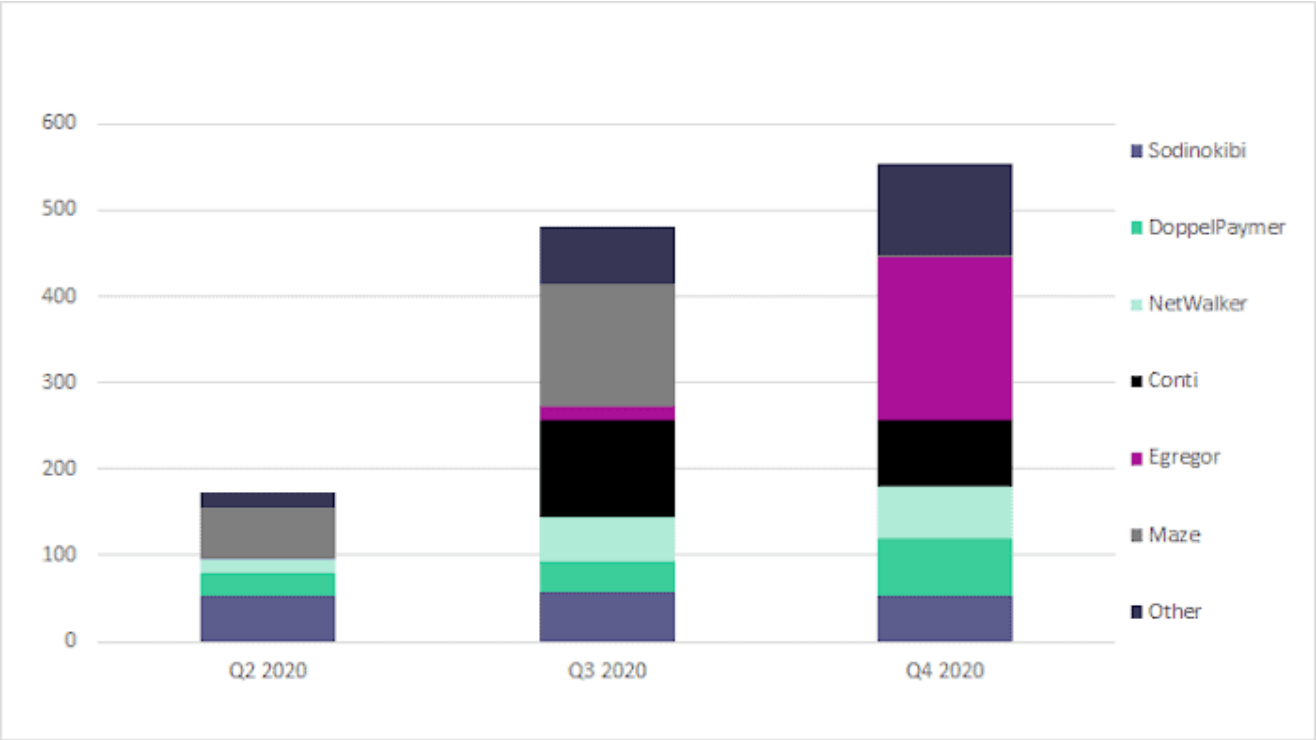
There has been a lot of talk regarding ransomware activity and groups throughout 2020—who was most active, big targets that were hit, and on and on. Of the ransomware data leak sites we monitor, six groups made up 84% of our alerts—Maze, Egregor, Conti, Sodinokibi, DoppelPaymer, and NetWalker.



Most popular ransomware blog locations in 2020, as reported in Digital Shadows Intelligence

While NetWalker and DoppelPaymer have remained consistent throughout the year in number of posts, Egregor entered the scene late in 2020 and hit the ground running, while Maze was about to exit the scene.

The “Other” ransomware data leak sites accounted for 16% of Digital Shadows’ alerts and consisted of Ako/Ranzy Locker, Avaddon, Clop, DarkSide, Everest, LockBit, Mount Locker, Nefilim, Pay2Key, PYSA, Ragnar Locker, RansomEXX, Sekhmet, and SunCrypt.

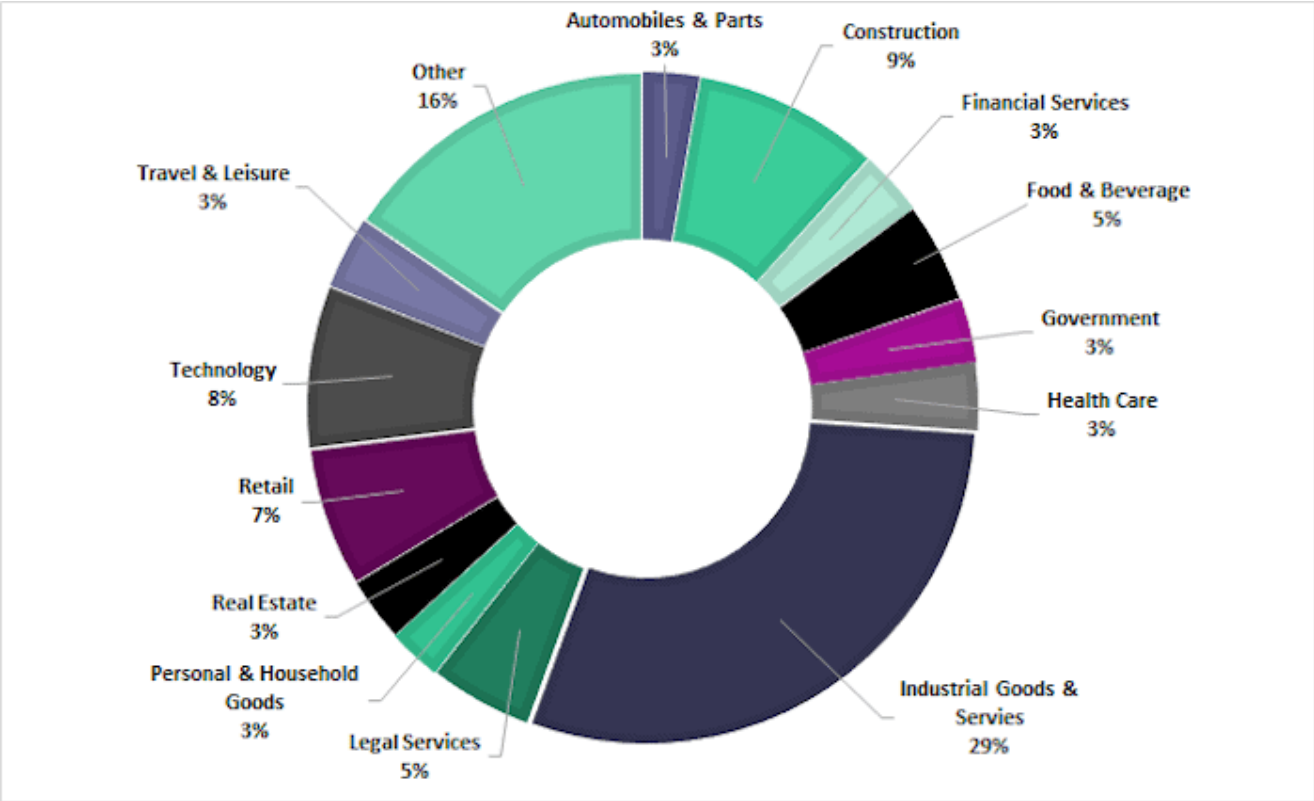


Distribution of ransomware blog sites across Q2, Q3, and Q4 2020, as reported in Digital Shadows Intelligence

What was the most targeted industry by ransomware operators in 2020?

Ransomware operators targeted organizations in various sectors, and it didn't appear any sector was off limits to these groups. Industrial Goods & Services was the most targeted industry, accounting for 29% of our alerts, while the remaining were split among several sectors.

Industrial Goods & Services was the most targeted industry by ransomware operators in 2020. (*Digital Shadows research)*

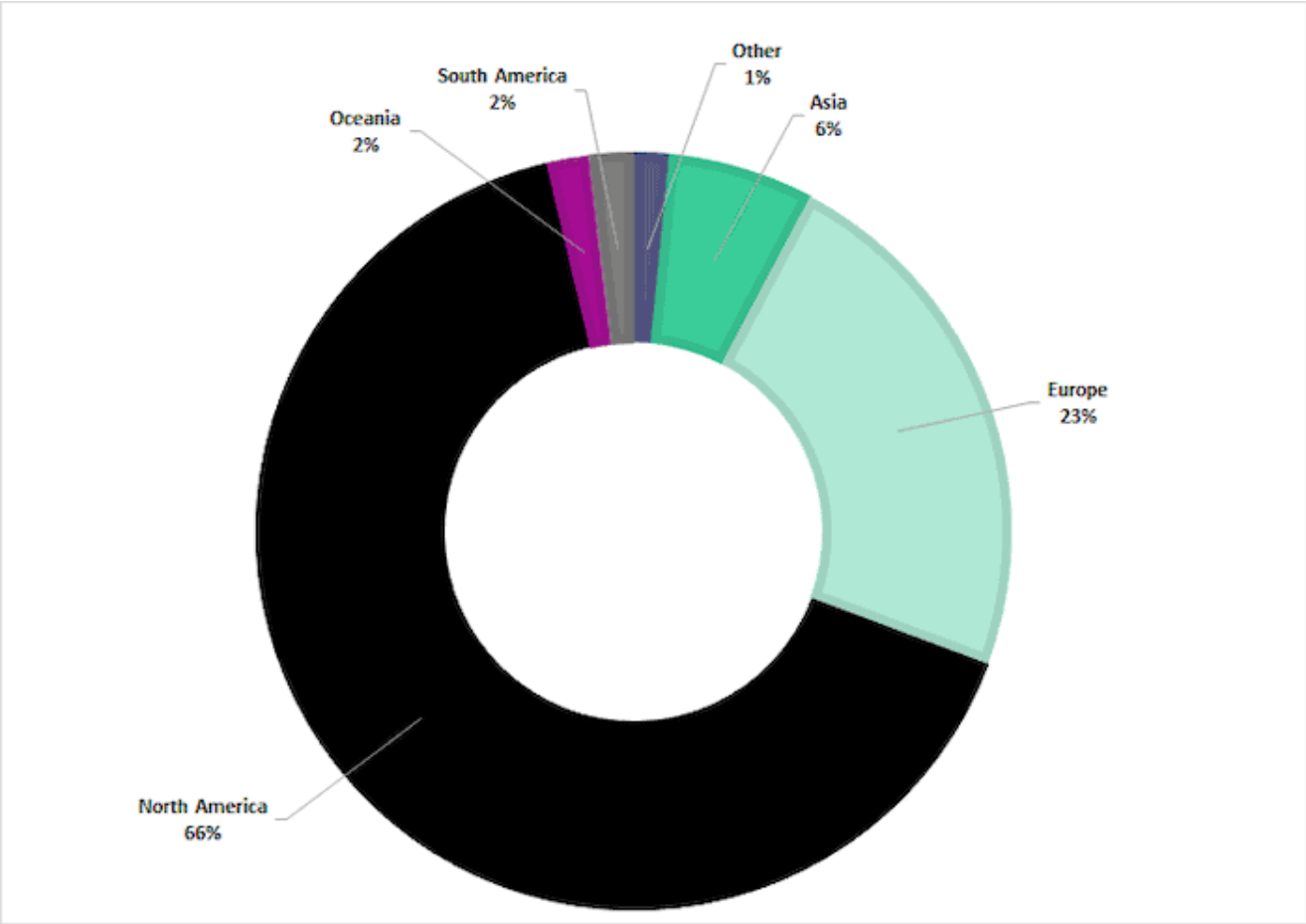


Breakdown of targeted sectors on ransomware data leak sites throughout 2020, as reported in Digital Shadows Intelligence

"Other" sectors accounted for 16% of Digital Shadows' alerts and consisted of aerospace, banks, basic resources, chemicals, conglomerates, consulting services, cyber security, defence, education, energy, equity/non-equity investment instruments, hospitality, insurance, law enforcement, media, NGO, oil & gas, pharmaceuticals, religious, telecommunications, utilities, veterinary services, and waste management.

North America was the most targeted geographic region with 66% of our ransomware alerts coming from organizations in NA. (***Digital Shadows research)***

While ransomware groups did not appear to be biased when targeted sectors in 2020, the groups did appear to have a geographic preference.



Breakdown of target locations throughout 2020, as reported in Digital Shadows Intelligence
The other category made up 1% of our alerts reported in 2020 and consisted of countries located in Africa and The Carribean, which contained less than 10 incidents each.

Which ransomware operators started and stopped in 2020?

The “end” of Maze

On 01 Nov 2020, Maze Group operators posted a press release on their data leak site announcing an end to operations. Maze led our profile of high threat hacker groups in Q2 2020 and is known as the innovator of data leak sites.

In mid-March 2020, the Maze operators stated they would halt activity against all medical organizations until the end of the COVID-19 pandemic. However, in April, the group released data stolen from the drug testing firm Hammersmith Medicines Research Ltd (HMR). Although it appeared the group may have been faulting on their word, the group stated the data was encrypted and stolen prior to their announcement.

The announcement claimed that the group’s intent had been to bring light to security weaknesses and warned that cybercriminal could exploit these weaknesses to cause significant damage, even risking human life. Additionally, the group pledged to return to show

the world it's "errors and mistakes". While we don't know why the group officially ceased their operations, it is possible the oversaturation of the ransomware market motivated their exit.

The rise of Egregor

Egregor ransomware was identified in September 2020, and is believed to be closely related to the Sekhmet ransomware variant. Egregor's name is derived from Western occult traditions. Egregor is a term applied to the collective energy or force of a group of individuals united toward a common purpose.

Egregor ransomware's operators achieved recognition in October 2020 when they targeted US bookstore chain Barnes & Noble and video game producers Ubisoft and Crytek. Egregor entered the scene and made a name for itself— Egregor victims increased 240% from 25 September to October and another 43% from October to 17 November.

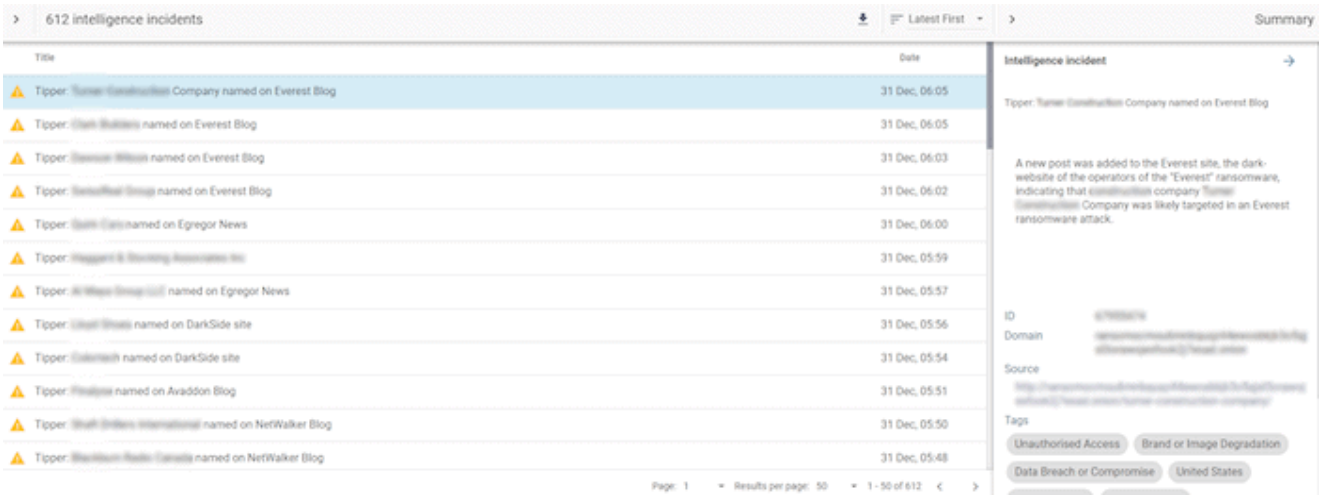
Reporting has suggested that operators of the Maze ransomware have shifted to using the Egregor ransomware variant; however, this has not been confirmed by either group. This theory is supported by the level of sophistication demonstrated by Egregor in a short time frame and Egregor's victimology is consistent with targeting conducted by the operators of the Maze ransomware variant.

What is to come in the ransomware threat landscape for 2021?

As discussed in our 2021 forecasts blog, the threat of ransomware attacks is likely to continue through 2021. The pay or get breached trend has proven successful since December 2019 and is likely to continue to attract ransomware groups. This tactic is likely to allow new or less known variants an opportunity to compete with some of the more successful variants, such as Egregor, DoppelPaymer, NetWalker, and Sodinokibi. Maze may have exited the ransomware scene, but there are plenty of ransomware groups waiting to take the number one spot (Egregor, we see you).

In 2020, we witnessed costly attacks reported every day that crippled companies in every industry; in 2021 we encourage and hope to see private and public organizations better mitigating this threat.The best security teams will stay up to date with threat intelligence on the ransomware threat landscape to be able to identify data exposure on data dump sites early, research associated vulnerabilities, and identify early discussions and advertisements for sensitive information and employee credentials on cybercriminal marketplaces and forums.

Digital Shadows updates a threat intelligence library of over 400 threat actors, events, and campaigns here. Tracking, identifying, and keeping teams updated on ransomware groups, tactics, and trends in their industry vertical and geographic region, including actionable insights from ransomware trends, and assesses the risk certain actors post to your industry, company, and assets. Look here for a trial of our product SearchLight.



If you're a Digital Shadows client, you'll be able to use this search term to set up alerts on new instances of data dumps on ransomware sites: ransomware dumps.

Tags: Ransomware