COVEWARE

Global Ransomware Marketplace Report

Q4 2018

Follow us on twitter: @coveware
Read our blog: www.coveware.com/blog

About this report

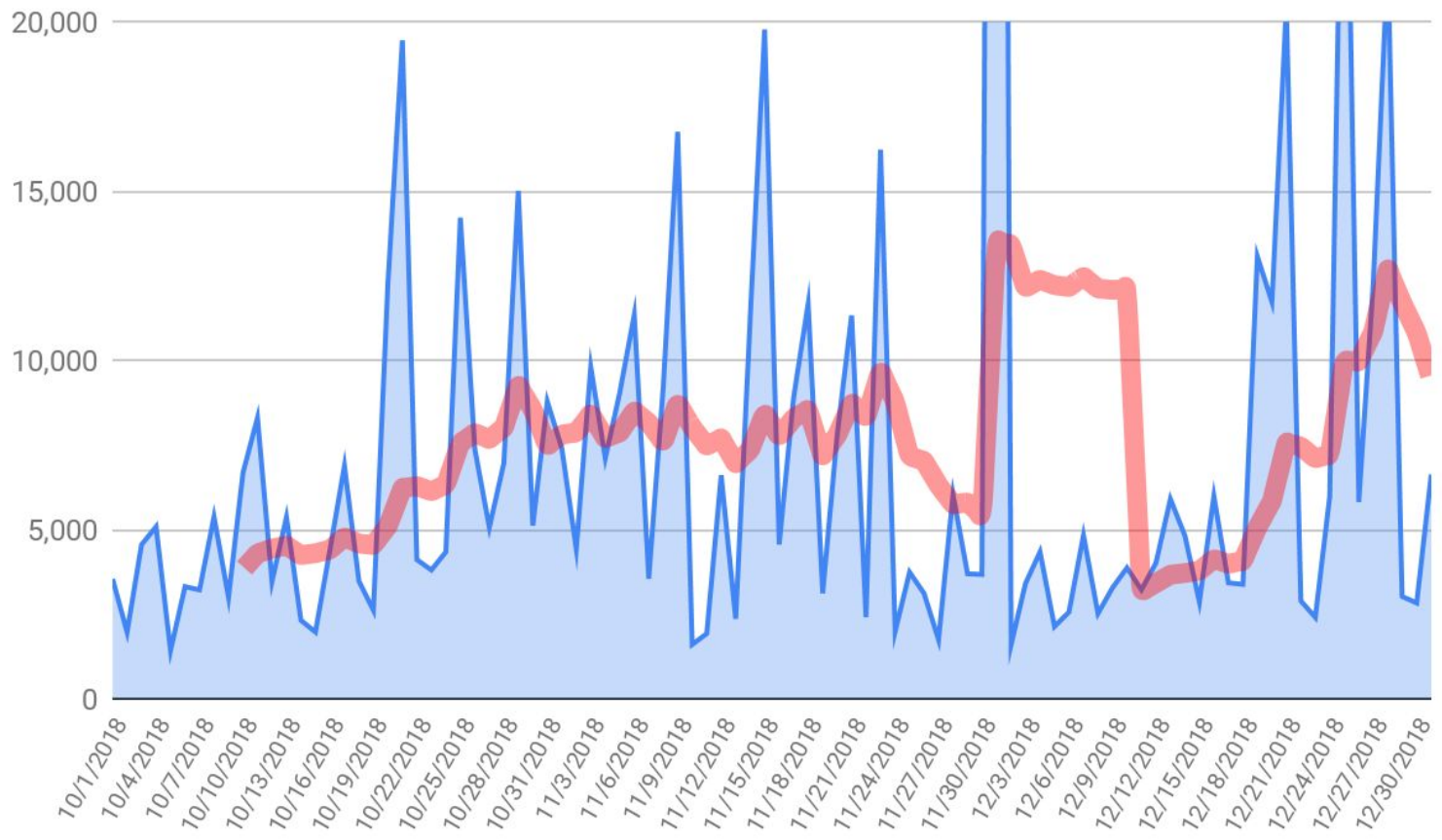
This report aggregates anonymized ransomware data from actual cases handled and resolved by the Coveware support team on the Coveware incident response platform. Unlike surveys, which rely on sentiment, this report is created solely from a standardized set of data collected from every case.

By aggregating data, and broadcasting our findings, Coveware believes enterprises large and small can better protect themselves from the persistent and ever evolving ransomware threat.

To learn more about this report, reach out to info@coveware.com or visit www.coveware.com

Average Ransom Amount: $6,733

Average amount paid per incident in Q4 of 2018



The average ransom increased by 13% as compared to Q3 of 2018 ($5,973).

Coveware suspects the increase reflects the more targeted nature of recent ransomware attacks. In Q4, ransomware distributors focused on larger targets and via bespoke RDP & social engineering attack vectors. Higher priced ransomware strains like SamSam and Ryuk also increased in frequency during Q4, despite the ubiquity of Dharma, GandCrab and GlobeImposter.

Ransomware Incident Duration

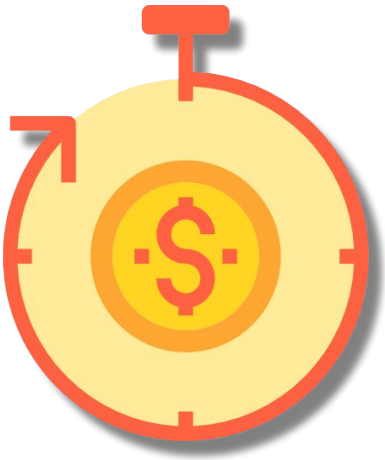
How much downtime is expected? How much did it cost?

6.2 days

Average number of days a ransomware incident lasts

$54,904

Average cost of ransomware incident related downtime



Average downtime increased by 47% over Q3, also reflecting the increasingly bespoke nature of the attacks. The increase in downtime was due to the frequency of attacks where backup systems were wiped or encrypted as part of the attack.

We estimated downtime costs by reviewing the location and the industry of the organization and using labor and margin statistics to estimated downtime costs per hour.

Top Ransomware Cryptocurrencies

Ransomware denominations of Q4 2018

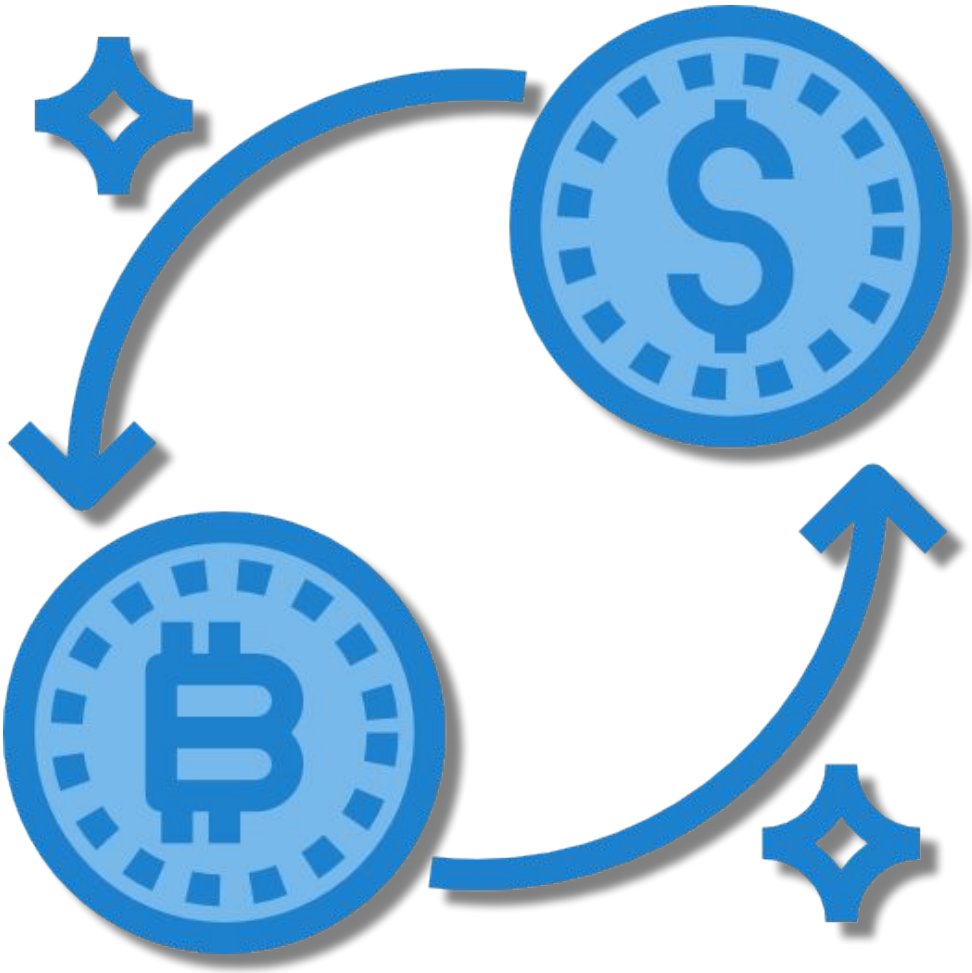
95% Bitcoin is still the most preferred cryptocurrency in ransomware.

5% Privacy coins like Dash are growing in use.

Bitcoin, despite its falling price in Q4, continues to be the preferred cryptocurrency for ransomware. While Bitcoin wallets are anonymous, the transactions are trackable. Gandcrab charges 10% more for ransomware if paid in Bitcoin vs Dash, which is known for its greater anonymity.

Payment Success Rate

When you pay, do you receive a decryption tool / keys?



93%

Payment Success Rate

93% of the time, paying the ransom results in a decryption tool. However, payment success rates vary dramatically based on ransomware type, and the victim company's negotiation and payment tactics.

For example, the GandCrab TOR site is very reliable and delivers a decryptor tool if you pay. However, some variants of Dharma can be much riskier depending on the variant and individual distributor.

Overall Data Recovery Rate

When you run decryption, how much data is recovered?

86%
Recovered

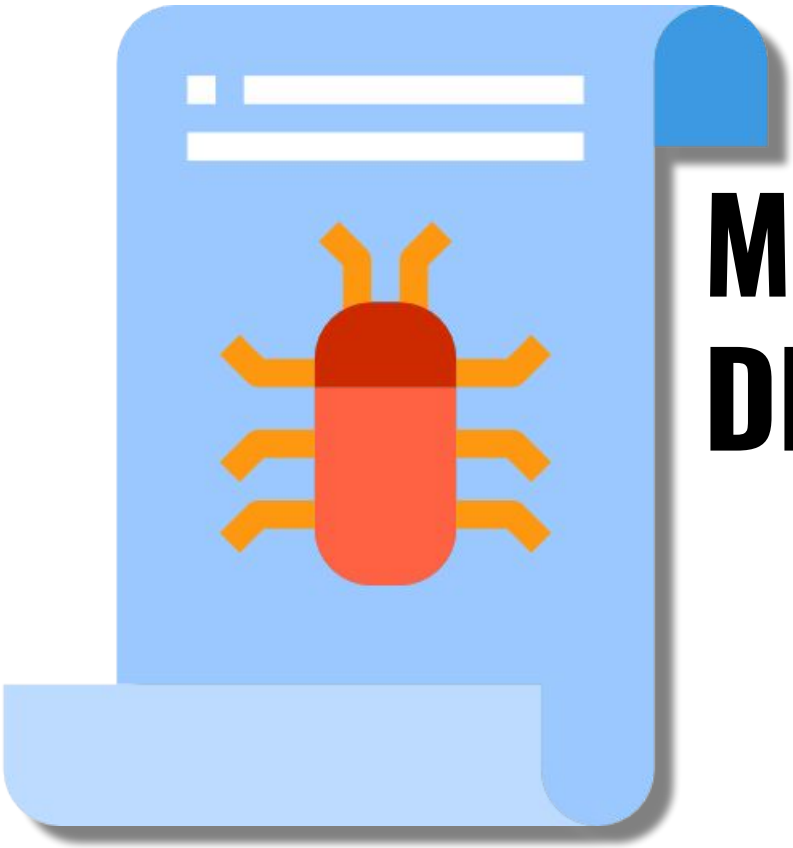
14%
Lost

When a victim of ransomware pays, they receive a decryption key 93% of the time, but that is just the beginning of the recovery process. Encryption can damage or wipe files, and sometimes the decryption tools do not work well.

The average data recovery rate when a working tool is delivered is about 95% but varies dramatically depending on the type of ransomware. For example, Ryuk is low at ~60%, while SamSam is close to 100%.

Most Common Ransomware Types

1. Dharma / CrySiS (multiple variants)
2. GandCrab 5.04+
3. Global Imposter 2.0



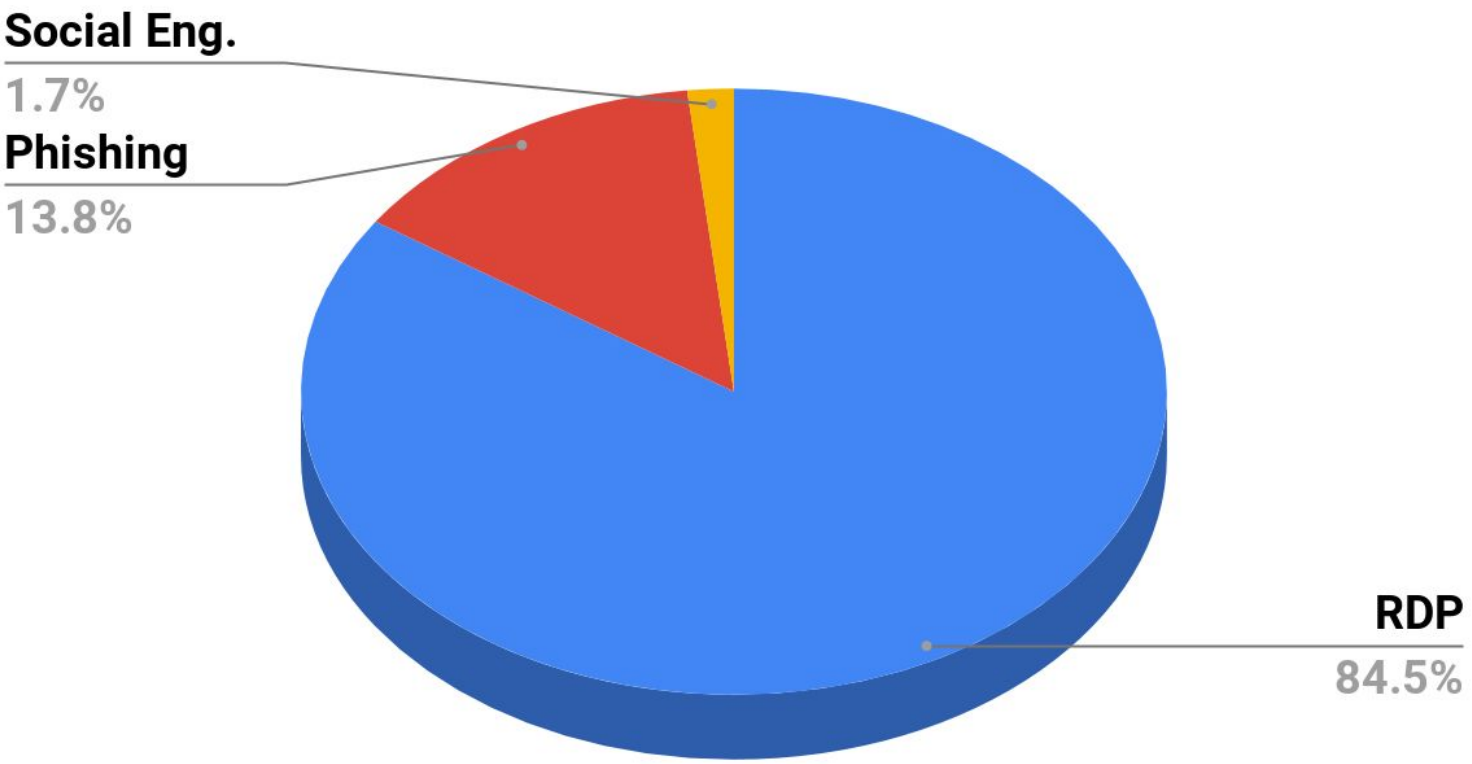
Most Common Dharma Variants

1. .adobe
2. .gamma
3. .combo

Dharma/Crysis was the most prevalent type of ransomware in Q4. Distribution and variants increased significantly as did payment defaults. Dharma extensions **.adobe and .gamma were the worst offenders** registering the most payment defaults out of any other ransomware type. We attribute this to the increased syndication to less sophisticated ransomware distributors during the quarter.

Top Ransomware Attack Vectors

What attack vectors were most commonly exploited?

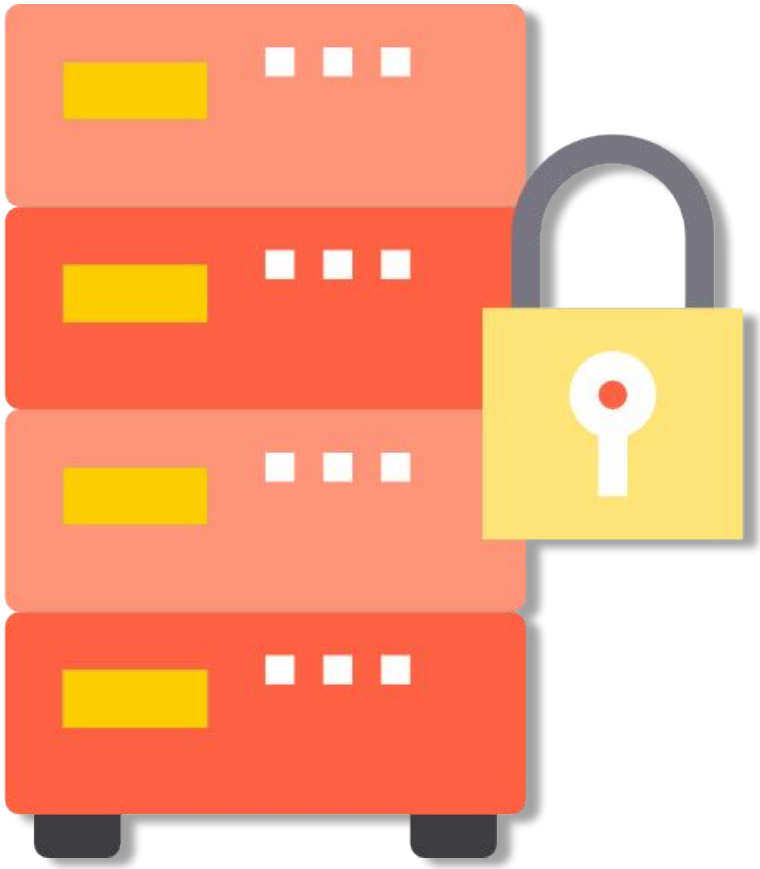


Remote Desktop Protocol (RDP) based breaches were AGAIN the most prevalent ransomware attack vector in Q4. Accordingly, ransomware distributors are spending increased time inside of breached networks. Admin credentials are harvested so backups can be wiped or encrypted, ensuring the attack has maximum impact.

We expect this attack vector to remain popular until the number of vulnerable targets shrinks.

Importance Of Backups

Did backups become encrypted during the attack?



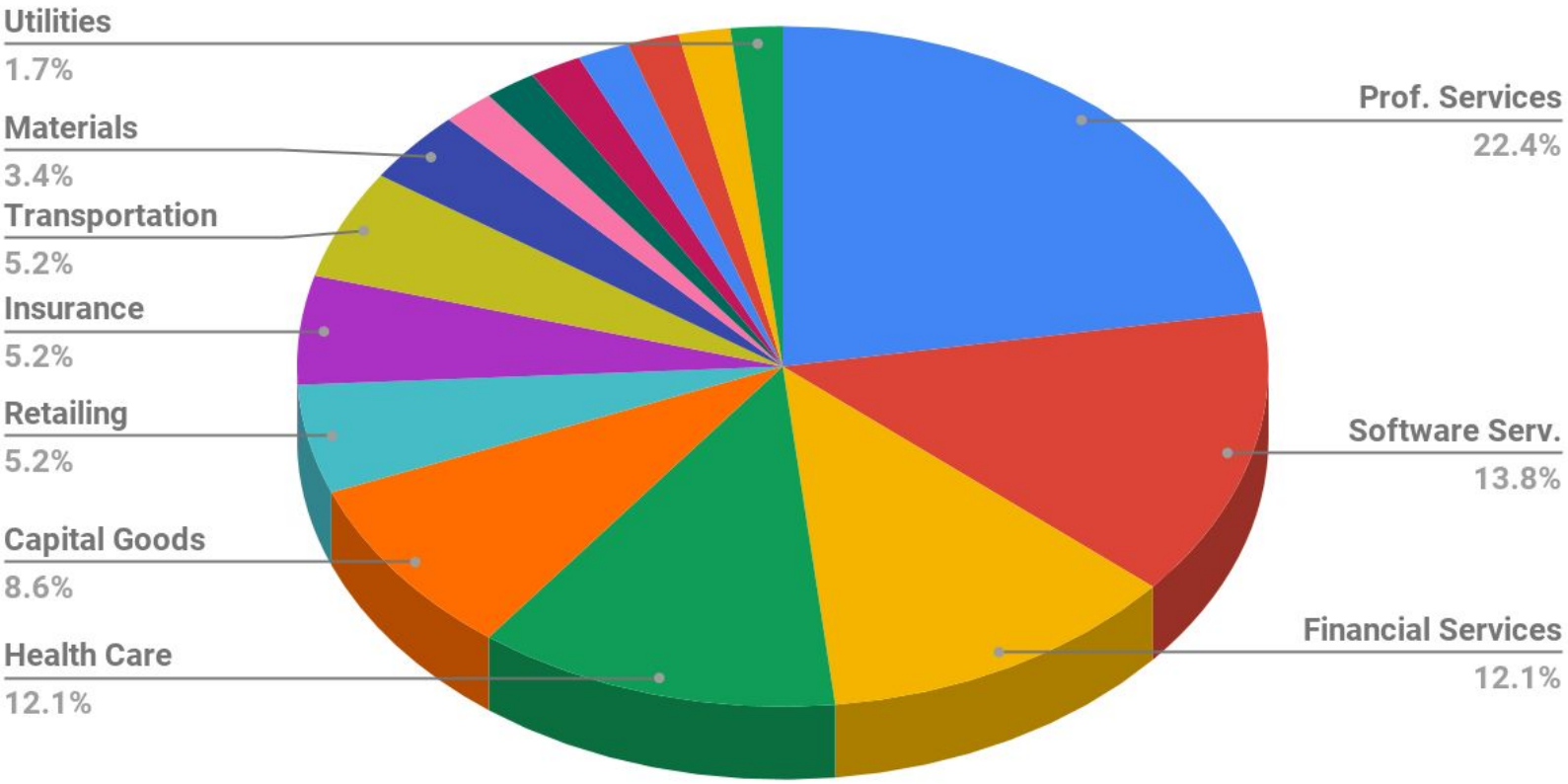
75%

of organizations that paid a ransom had their backups compromised.

The percentage of companies with compromised backups increased over 54% in Q3. This is consistent with the increasingly bespoke nature of ransomware attacks in Q4. Backup systems are typically the first target of the hacker. Next, hackers encrypt the primary file and application servers in order to completely cripple the target company. Proper network partitioning and 'least privilege' administrative access **are a must** to avoid being compromised.

Ransomware Demographics

How are industries targeted by ransomware?



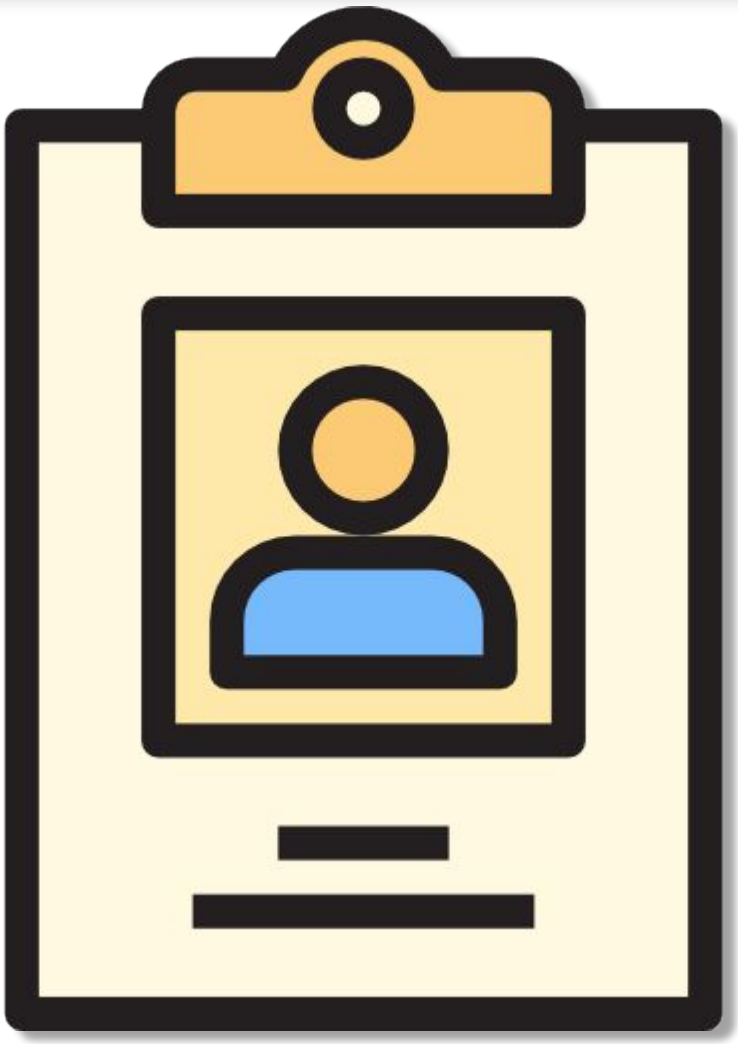
Note: Consumer Services,Media, Automobile, Technology Hardware & Equipment, Real Estate, & Food & Staples Retailing were all less than 1.5% of ransomware attacks

Professional service firms, such as regional law firms and CPA firms, continue to be a prime target for ransomware. These firms tend to under-invest in IT security, have weak or no backup policies, and have almost no tolerance for data loss.

We also observed an increase in local healthcare facilities being targeted. These attacks typically caused the facility to close their doors until critical scheduling and patient EMR servers could be recovered.

Ransomware Demographics

Average # of employees in a victim organization



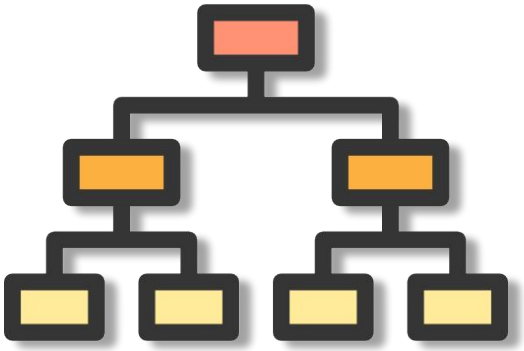
71

Employees

The average company size doubled to over 70 employees in Q4, up from 38 in Q3. This statistic compliments our observation that ransomware is becoming increasingly bespoke, targeting larger companies with more targeted attacks, and demanding higher ransoms.

Ransomware Demographics

IT staff at organizations that paid ransomware



49% In house

51% Outsourced

Ransomware attacks moved up market in Q4, and accordingly the profile of the victim company's IT staff shifted towards in-house, rather than outsourced.

Outsourced MSPs (Managed Service Providers) continued to be tested as both end clients, and break fix clients become targets.

Increased IT Security Spending

% of companies that increase their IT spending after having to pay for ransomware

70% of organizations that paid a ransom intend to increase their security spending to prevent future incidents

The percentage of companies that planned to increase their IT security spend following a ransomware attack increased in Q4. This likely reflects the larger profile of the average company and their ability to allocate budget to IT security spending.

Disclaimer & Other Notes

Coveware is not responsible for any actions taken, errors or omissions (negligent or otherwise), regardless of the cause, or for the results obtained from the use of this content, or for the performance of any computer, hardware or software used or modified in conjunction with this content. The content is provided on an "as is" basis.

VIEWERS OF THIS REPORT AND ITS CONTENT DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

In no event shall Coveware be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the content even if advised of the possibility of such damages.

Some images designed by ITIM2010 from Flaticon.

