COVEWARE

Global Ransomware Marketplace Report

Q3 2018

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

About this report

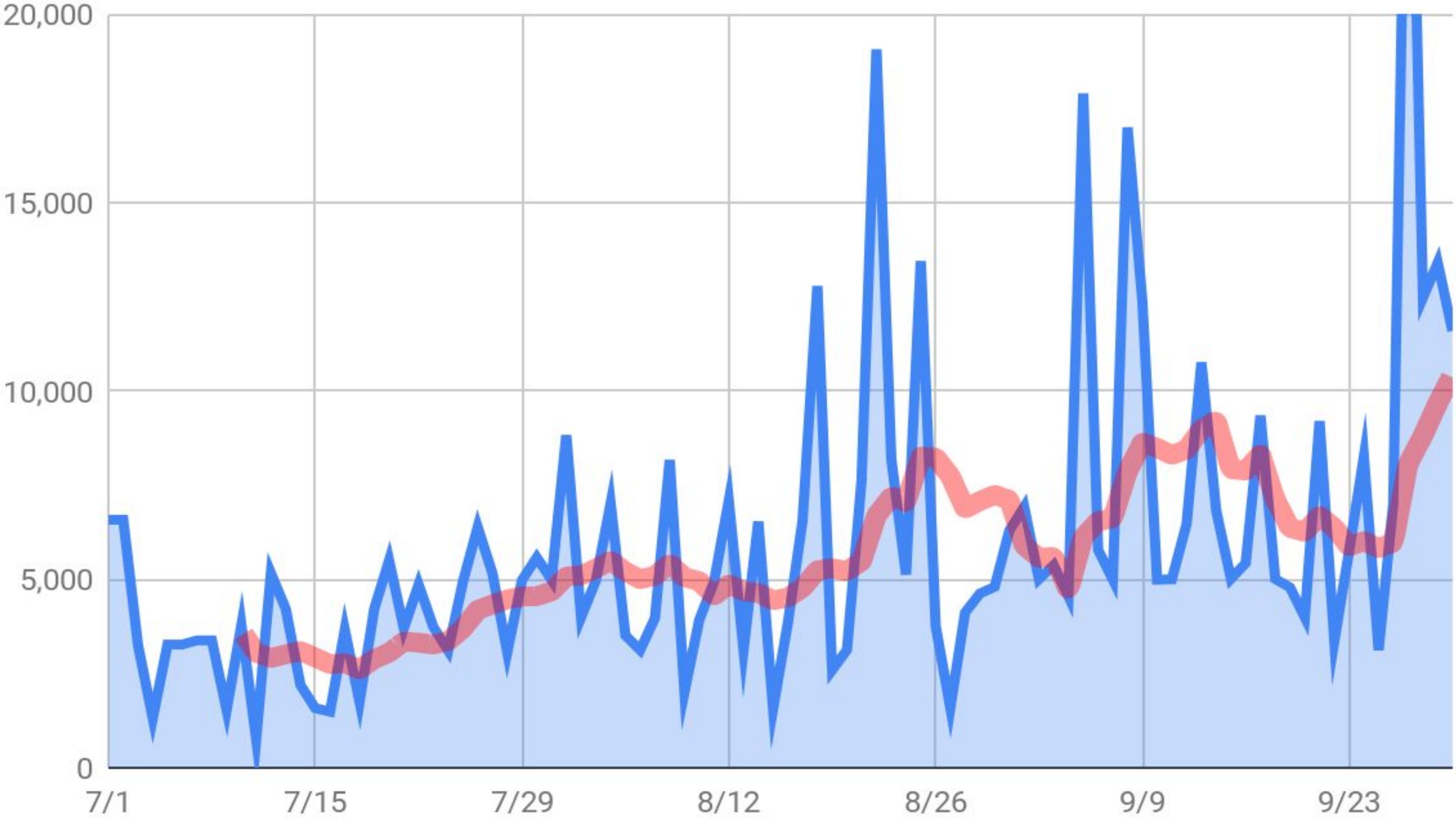
This report aggregates anonymized ransomware data from actual cases handled and resolved by the Coveware support team on the Coveware incident response platform. Unlike surveys, which rely on sentiment, this report is created solely from a standardized set of data collected from every case.

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: $5,974

Average amount paid per incident in Q3 of 2018



The average ransom demonstrate the hacker's understanding of the business value of encrypted data (median amount was $4,983). Through our negotiations it is clear that hacker groups are taking detailed notes on the size and type of the machines they encrypt along with the size of the organizations. Ransom amounts are scaled accordingly.

At the same time, we fielded cases from small businesses in Argentina that unfortunately had no hope of paying the ransom given the recent devaluation of their currency...so not all hackers were paying attention.

Ransomware Incident Duration

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

4.2 days

Average number of days a ransomware incident lasts

$36,586

Average cost of ransomware incident related downtime

Ransom amounts are immaterial as compared to the costs of downtime. Ransomware can bind up the operability of an organization and severely limit, if not cripple operations. 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 Q3 2018

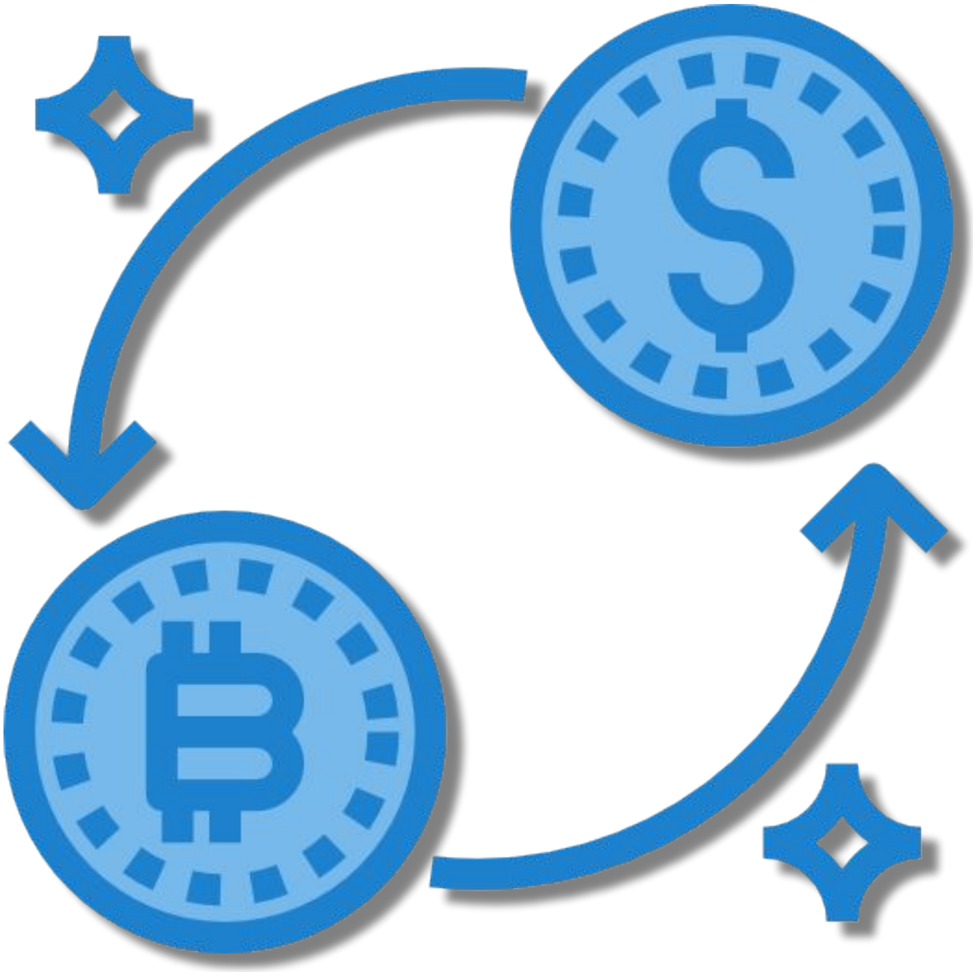
98% Bitcoin is still the most preferred cryptocurrency in ransomware

2% Privacy coins like Dash are growing in use.

In tracking payments made to wallets used in ransomware, we note heightened use of mixers to obfuscate the destination of aggregate collections. Hackers are also crossing bitcoin into these more opaque privacy coins as part of the obfuscation process given the ability of bitcoin to be traced back to exchanges.

Payment Success Rate

What % of ransomware payments resulted in delivery of a decryption key?



100%

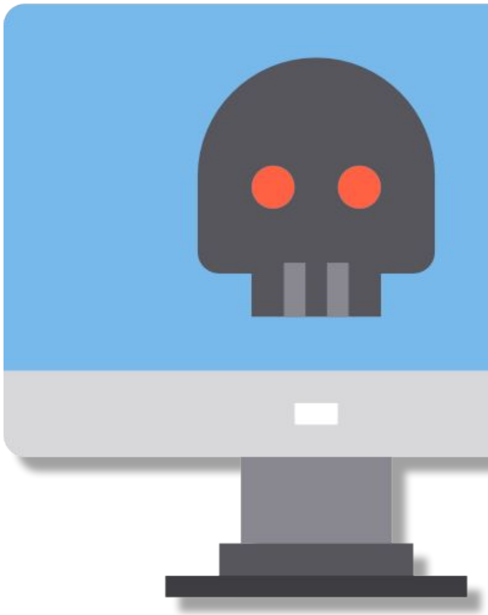
Payment Success Rate

Most security industry reports blur this metric with data recovery. Either way, neither approach 100%. Our payment success rate is a function of properly identifying wiper malware vs. ransomware, and by rigorously profiling the hacker prior to a counterparty making a payment.

We do not expect this rate to remain at 100% forever, but it will remain our target.

Data Recovery Rate

How effective was the decryption tool at recovering data?



99.6%

Recovered

0.4%

Lost

The efficacy of a ransomware decryptor tool matters just as much as payment success. While the tools provided can be difficult to use, and the instructions provided by the hacker even worse, counterparties find a way. The data recovery rates are much higher than as reported by other anecdotal, and sentiment based surveys. Lost data is normally attributed to file corruption as a result of the encryption process.

Most Common Ransomware Types

1. Dharma / CrySiS
2. GandCrab
3. Global Imposter

Most common Dharma variants

1. .combo
2. .bip
3. .gamma

When ransomware encrypts a file, it appends a unique file extension to the file’s name. This file extension is used to identify both the ransomware type and the variant of the type. Different variants can indicate new versions of the ransomware or a different hacker group that is distributing it.

Top Ransomware Attack Vectors

What attack vectors were most commonly exploited?

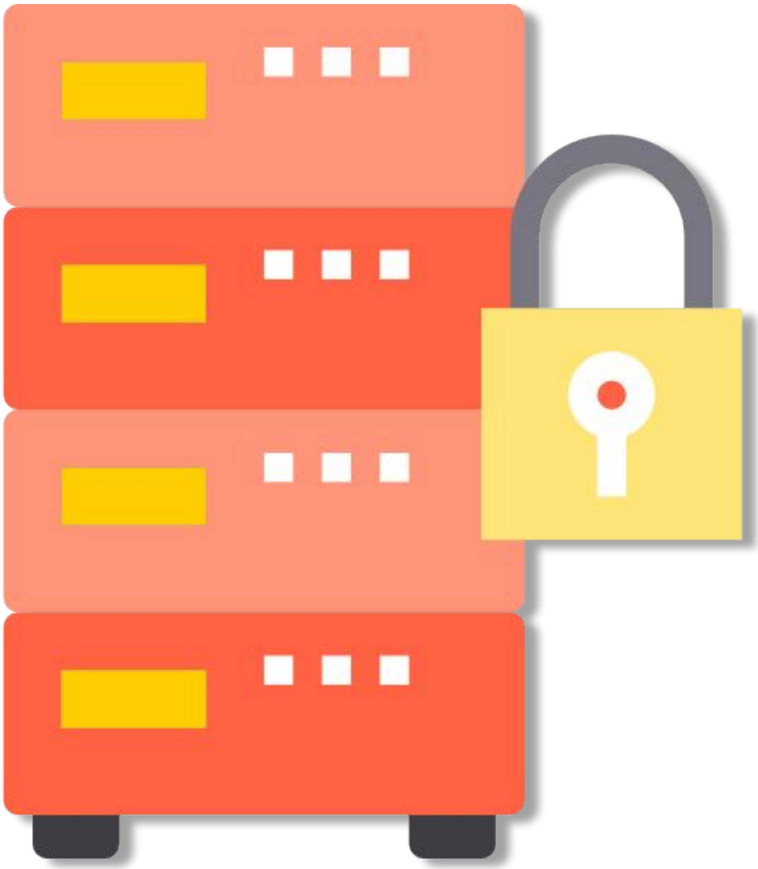
#1 Remote Desktop Protocol

#2 Email phishing attacks

Remote Desktop Protocol (RDP) remains the favorite attack vector for ransomware hackers. Email based attacks remain popular, but the availability of cheap exploit kits and previously breached credentials on dark secondary markets make intrusion more accessible. Additionally, the ability to proliferate ransomware across partitioned networks, and backups has made RDP a favorite target.

Impact of having backups

How helpful were backups to organizations that paid ransom?



54%

of organizations that paid a ransom had their backups compromised.

Data backups are always the first avenue for recovery when ransomware occurs. Despite the prevalence of backups, a large proportion of companies that paid a ransom did so because their backups become compromised in the attack.   Hackers are increasingly targeting the backup systems that both store and manage access to data copies in ransomware attacks.

Ransomware Demographics

Industries most susceptible to ransomware in Q3 2018

#1 Commercial Services

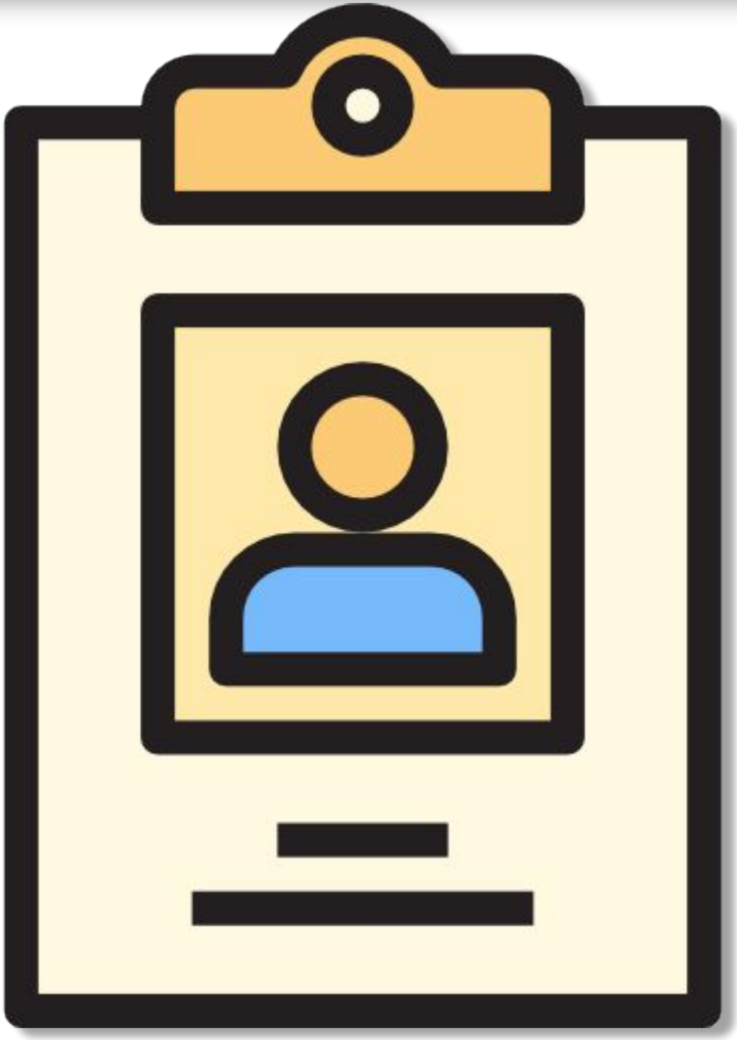
#2 Capital Goods

#3 Healthcare services

Industries that are commonly targeted by ransomware hackers combine a mixture of companies where data preservation is federally regulated (high value, highly likely hood of paying) and poorly secured (easy to break in). The top three industries represent a blend of high business value data such as Law Firms and Healthcare and poorly secured industrial companies, mainly construction and heavy industry.

Ransomware Demographics

Average # employees in an organization that paid a ransom



38

Employees

The average company hit with ransomware had 38 employees. This highlights this issue as predominantly an issue for small and medium sized businesses. These businesses do not have the budget for the latest security tools, but are also at greive risk of insolvency if the ransomware incident can not be resolved quickly.

Ransomware Demographics

IT staff at organizations that paid ransomware

36% In house

64% Outsourced

The majority of companies that have been hit with ransomware have external or outsourced IT. Of these, most are not using a fully managed outsourced provider such as IT managed service provider (MSP) or managed security service provider.

Increased IT security spending

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

64% of organizations that paid a ransom intend to increase their security spending to prevent future incidents

This number should be 100%, but sadly it is not. Still, most companies that become the victim of a ransomware attack increase their IT spending budgets immediately afterwards.

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.