# Ransomware attacks surge and ransom demands rise

In recent months, Beazley Breach Response (BBR) Services has seen the number of reported ransomware incidents climb again. The varieties of ransomware and the differing technical abilities of the criminals make effective response especially challenging. Breach response services, such as forensics and legal counsel, are often necessary in ransomware attacks to determine the attack vector and level of access obtained by the attacker. If the attacker accessed or exfiltrated personally identifiable information or protected health information, notification to affected individuals may be required by law.

In September, our insureds were hit particularly hard, with notifications to Beazley of ransomware attacks more than doubling relative to August. It is unclear if this spike will continue, as up until September the overall number of ransomware incidents in 2018 have been holding steady with 2017 numbers. Healthcare is still the most targeted industry (37%). The next hardest hit sector was professional services (11%). In Q3, financial institutions saw an 18 percentage points increase in ransomware attacks over the previous quarter.

Criminals are employing a wide range of ransomware variants, including Dharma, GandCrab, Ryuk, and BitPaymer. These variants are spread in different ways. Dharma appears to be launched manually after the criminal exploits remote desktop protocol (RDP). GandCrab is spread through malvertising that directs a user to a site infected with an exploit kit. The kit exploits vulnerabilities in Adobe Flash Player or the Windows VBScript engine to install the malware.

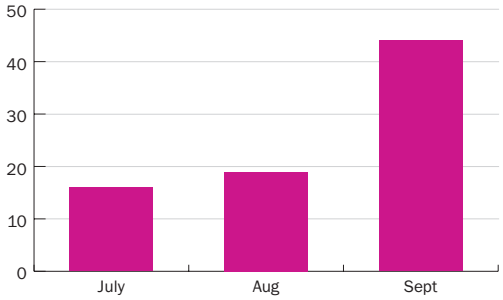
Ryuk and BitPaymer have been associated with some of the highest ransom demands. Kivu Consulting has reported that the BitPaymer ransomware is appearing on systems that have also been infected with banking Trojans - malicious programs used to obtain confidential information of customers using online banking and payment systems. In July, the United States Computer Emergency Readiness Team (US-CERT) issued a warning about one banking Trojan in particular, Emotet, which is spread through phishing and possesses sophisticated capabilities to download other malware.

Successful decryption of ransomed data has also become more challenging. Winston Krone, global managing director of Kivu Consulting, describes “a sharp increase in ‘bad’ ransomware strains – where the malware carries out the encryption but has poor functionality, fatally corrupts substantial portions of the victim’s data, fails to decrypt properly after payment of a ransom, or is favored by volatile, unskilled attackers who are unable to troubleshoot decryption issues.”*

In the more sophisticated attacks, we have also seen ransom demands increase significantly, up to as high as $2.8 million. In these instances, criminals have either targeted the victim organization or upon obtaining access discovered that they had more leverage and therefore increased the ransom demand. They’ve also done reconnaissance on the victim’s network and compromised back-ups before deploying the encrypting malware, which puts pressure on the organization to pay the ransom.

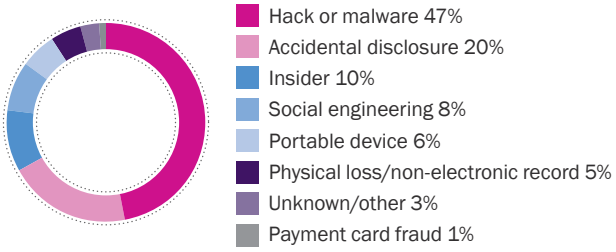
In the first nine months of 2018, 71% of ransomware incidents handled by BBR Services impacted small and medium-sized businesses. There are likely several explanations for the high percentage. First, larger companies often have more resources to put better controls in place to prevent ransomware from coming in or spreading throughout the network. Second, smaller companies are less likely to have properly segmented their backups, resulting in a higher likelihood that they will need to pay the ransom to get back up and running. Additionally, larger companies may have viewed the WannaCry and Not Petya worldwide attacks as wakeup calls and implemented better system patching protocols.

### Increase of ransomware attacks in Q3




The top two causes of data breaches reported to BBR Services in 2018 were hack or malware attacks (47%) and accidental disclosure (20%). Hack or malware, which also includes ransomware, is up 11 percentage points compared to the same period in 2017. This is due to a sharp increase in the number of email compromises in 2018.

### Causes of incidents, 2018



CBSL565_US_10/18

## Breaches by industry

Business email compromise incidents continue to rise and have more than doubled in the first nine months of 2018 compared to the same period in 2017. The attacks continue to be broadly distributed across industry sectors, including healthcare, financial services, professional services and higher education.

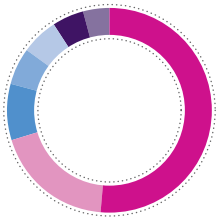
**Higher education**
Hack or malware incidents were up 7 percentage points from the same period in 2017 to 52% of the total number of incidents for higher education institutions. Social engineering incidents also increased 4 percentage points, while accidental disclosure numbers fell 9 percentage points. The increase in social engineering incidents is due to an increase in fraudulent wire instructions.

**Financial services**
The number of hack or malware incidents reported to BBR Services in 2018, Q1-Q3 increased 5 percentage points compared to 2017. However, accidental disclosure incidents decreased 6 percentage points.

**Healthcare**
Accidental disclosure (32%) leads the causes of incidents in healthcare despite a 11 percentage points drop from the same time in 2017. Hack or malware reports increased from 20% to 30% in the course of a year.

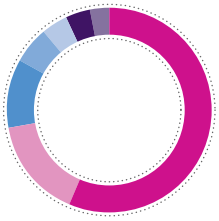
**Professional services**
Social engineering incidents (3%) have decreased 14 percentage points in 2018, while the number of hack or malware cases reported by professional services increased 7 percentage points.

### Higher Education Incidents, 2018



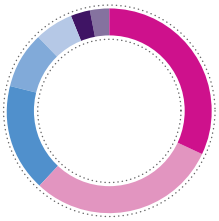
- Hack or malware 52%
- Accidental disclosure 19%
- Portable device 9%
- Insider 6%
- Unknown/other 5%
- Social engineering 5%
- Physical loss/non-electronic record 4%

### Financial Services Incidents, 2018



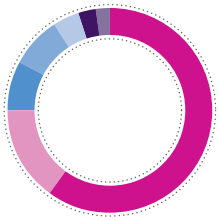
- Hack or malware 57%
- Accidental disclosure 16%
- Social engineering 11%
- Insider 6%
- Portable device 4%
- Physical loss/non-electronic record 4%
- Unknown/other 3%

### Healthcare Incidents, 2018



- Accidental disclosure 32%
- Hack or malware 30%
- Insider 17%
- Physical loss/non-electronic record 9%
- Portable device 6%
- Social engineering 3%
- Unknown/other 3%

### Professional Services Incidents, 2018



- Hack or malware 60%
- Social engineering 15%
- Accidental disclosure 8%
- Portable device 8%
- Unknown/other 4%
- Insider 3%
- Physical loss/non-electronic record 2%

## Case study

On a Friday evening, Beazley received a phone call from a policyholder that their systems were down, which compromised hundreds of servers. At the time the policyholder, a multinational business with global operations, reported ransomware but did not know the demand amount. They had contacted BBR Services to coordinate a provider to get their systems back up and running as soon as possible. BBR Services immediately brought in computer expert services to help with data restoration and a forensics expert to assure there was no third party access to the data.

On Sunday the company learned the ransom demand of $1.75 million, which they considered paying. Within the first 24 hours, BBR Services connected the policyholder with a crisis management firm and within the first 48 hours worked with the CFO to coordinate a back-up plan in case they were to pay the ransom.

The company ultimately decided not to pay the ransom. Computer expert services had the company up and running a week later and operations were fully restored. BBR Services also coordinated legal services and no notification was ultimately required.

## About Beazley's BBR Services Team

Beazley has managed thousands of data breaches since the launch of Beazley Breach Response in 2009 and is the only insurer with a dedicated in-house team focusing exclusively on helping clients handle data breaches.

The BBR Services team works directly with BBR insureds during all aspects of incident investigation and breach response and coordinates the expert services that BBR insureds need to satisfy legal requirements and maintain customer confidence. In addition to coordinating data breach response, BBR Services maintains and develops Beazley's suite of risk management services, designed to minimize the risk of a data breach occurring.

* Source: https://kivuconsulting.com/cyber-insurance-ransomware/

beazley

www.beazley.com/bbr