Sextortion and the dark side of the web

Opportunistic cyber criminals are engaging in a new, darker strain of social engineering by attempting to blackmail recipients into paying crypto-currency ransoms using so-called "sextortion" tactics.

A typical case of sextortion investigated by Beazley Breach Response (BBR) Services involves an email from someone claiming to have accessed the recipient's work computer and found the addresses of pornographic websites they have viewed. The sender says they have simultaneously recorded footage of the recipient as they watched these sites using their webcam, and threatens to share the recordings with their email contacts if their demands are not met.

The emails often contain a link or zip file they claim contains evidence of the internet or webcam activity, or to a website to pay the crypto-currency ransom. If clicked on, the link may in fact spread malware that can steal information and install GandCrab, a common ransomware used by hackers to lock-up the computer until the ransom is paid.

In the cases seen by BBR Services, assertions that the sender has compromising information have proved to be hoaxes. There is no sign yet that the targets of sextortion are anything other than random and it often turns out that no data has been compromised.

However, a small number of emails sent out to thousands of recipients may indeed hit home. If these individuals did engage in inappropriate behavior on their work computer, they could be vulnerable to extortion. When the first trickle of sextortion claims were reported to BBR Services in the summer of 2018, they took the form of spam campaigns aimed at credit unions, but since then, policyholders from various industries have been hit.

In the fourth quarter of 2018, BBR Services was notified of these cases by several policyholders involving demands for crypto-currency worth hundreds or thousands of dollars. To increase the authenticity of the demand, in some cases, the threatening email will include an old password linked to the recipient's email address. Such information is often obtained via the dark web where hackers dump and sell user credentials that have been compromised in earlier data breaches.

Messages containing the recipient's password potentially pose a larger security concern for businesses, especially as passwords are often recycled or only slightly changed by users. The issue can be further complicated if the email appears to come from another email address within the same organization. This can indicate a wider problem than a single, apparently random, phishing attempt.

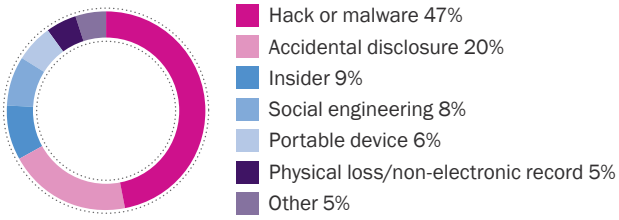
BBR Services has also seen advanced spoofing in connection with sextortion, where the email appears to be from the victim's own email account and it takes some investigation to determine whether or not the account was actually compromised.

It remains extremely important to scrutinize the source of any such email and to ensure that practical measures are being taken by employees to prevent an incident escalating into a wider issue. At an organizational level, businesses should ensure their domains are locked down to make it harder for external users to spoof domains under their control.

As with any cyber incident, if an employee reports receiving one of these emails, organizations should notify BBR Services and take sensible precautions to protect themselves. These include:

- Warning employees about this risk, mindful some may be reluctant to report it because of the potentially embarrassing nature of the threat
- Resetting an employee's password to minimize any risks from password recycling
- Enforcing strong password policies and educating employees about the risks of recycling passwords for different applications
- Setting up a multi-factor authentication process for remote access to email and other applications
- Regular employee training on how to identify phishing.

Incidents by cause, 2018



Cyber criminals targeted businesses of all sizes across industries in 2018. All sectors saw an increase in hack or malware incidents, largely owing to the 133% increase in business email compromises (BEC). Incidents of unintended disclosure fell across industries, likely as a result of the increase in hack or malware. Insider-led incidents were either stable or marginally higher in 2018 compared to the previous year.

CBSL585_US_02/19

Breaches by industry

Higher education

Of the incidents reported to BBR Services in 2018, 10% were in higher education. Of those, 50% involved hack or malware attacks, (mostly BEC) which is a 5 percentage point increase compared to 2017. Unintended disclosure was the other significant cause of loss at 21%. These are often emails sent to the wrong recipients, mailings gone awry, and file shares with sensitive information accidentally left open.

Financial services

Financial institutions' incidents accounted for 20% of those reported to BBR Services in 2018. 59% of these were hack or malware, up 7 percentage points from 2017. Unintended disclosure fell by the largest margin from 23% in 2017 to 15%.

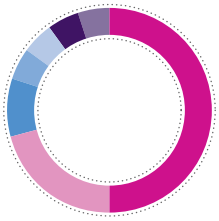
Healthcare

At 41%, healthcare entities reported the highest number of incidents of any sector. The most significant related to hack or malware and unintended disclosure – both accounting for 31% of overall reported healthcare incidents. This compares to 20% and 43% respectively in 2017. As with other industries, the increase in hack or malware and decrease in unintended disclosure is directly related to the massive increase in BEC incidents.

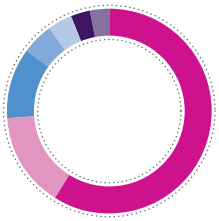
Professional services

Social engineering incidents fell to 13% of reported incidents from 19% in 2017, while hack or malware incidents increased by 9 percentage points to 59% of the overall portion. Overall, professional services attacks made up 7% of all those reported to BBR Services in 2018.

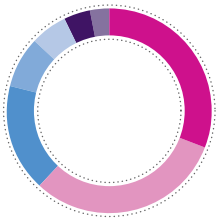
Higher Education Incidents, 2018



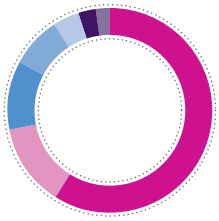
Financial Services Incidents, 2018



Healthcare Incidents, 2018



Professional Services Incidents, 2018



Case study

An employee of a Midwestern municipality was the recipient of an email from a cyber criminal claiming to have compromised their computer and accessed records of salacious website activity and control of the webcam. To bolster the credibility of the threat, the attacker included the purported hacked password as well as a link to download a zip file which they claimed contained a recording of the employee via their webcam. In reality, it contained an executable that installed malware onto the computer, specifically GandCrab ransomware. The ransom note demanded approximately $5,000 in Bitcoin. BBR Services coordinated the response, which included privacy counsel and computer forensics. Fortunately, the municipality was able to recover from recent backups, so it did not need to pay the ransom, and only lost a few days of non-critical data. After a thorough investigation, there was no evidence of access or exfiltration of sensitive personal information, and counsel was able to determine that there was no breach and notification was not 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.

beazley

www.beazley.com/bbr