Cyber Threat Insights

Second Issue, March 2018

*Welcome to the second installment of **Aon Benfield Cyber Practice Group's** Cyber Threat Insights newsletter. As always, the aim of this publication is to equip readers with relevant trends for cyber underwriting and portfolio management, based on the latest developments in the threat landscape. We hope Cyber Threat Insights is as informative to veterans of cyber insurance as it is to novices, providing visibility into an inherently murky environment.*

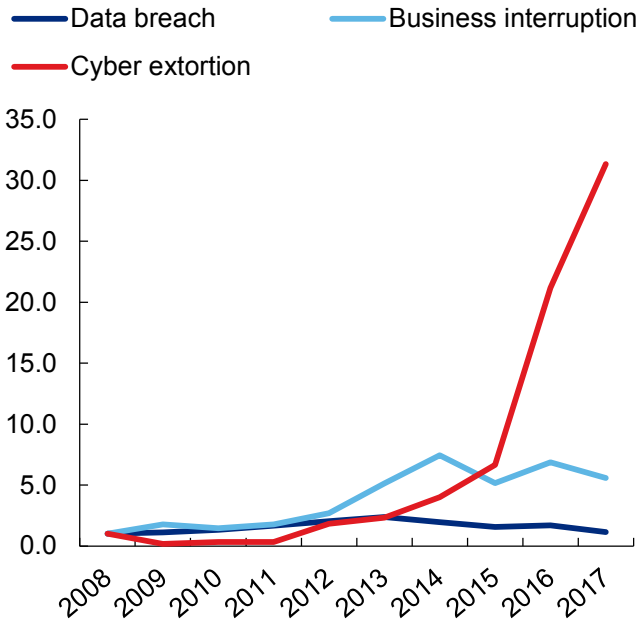
Cyber incident trends

Through the fourth quarter of 2017, cyber extortion rates remain elevated relative to other cyber incidents.

Based on our analysis reflected in exhibits 1 and 2, the rate of business interruption and extortion incidents continued to increase during the fourth quarter (exhibit 1). In fact, despite a significant reporting lag, the total number of cyber extortion events recorded for 2017 *already* exceeds the total tallied from 2016 (exhibit 2). We expect the 2017 number of extortion events to significantly eclipse 2016 totals, with no reason to believe this trend will abate in 2018. The security and financial environment dictates extortion will remain a burden for insureds and insurers for the foreseeable future.

The high volume of ransomware attacks continued into the fourth quarter, accounting for over 50 percent of malicious message traffic and malware observed by security experts during the period. And, unsurprisingly, the perpetrators overwhelmingly favored social engineering techniques over exploit kits, a trend that continued from the third quarter. Along with social engineering, malicious URLs sent via phishing, and strategic web compromise remained the preferred infection vectors.

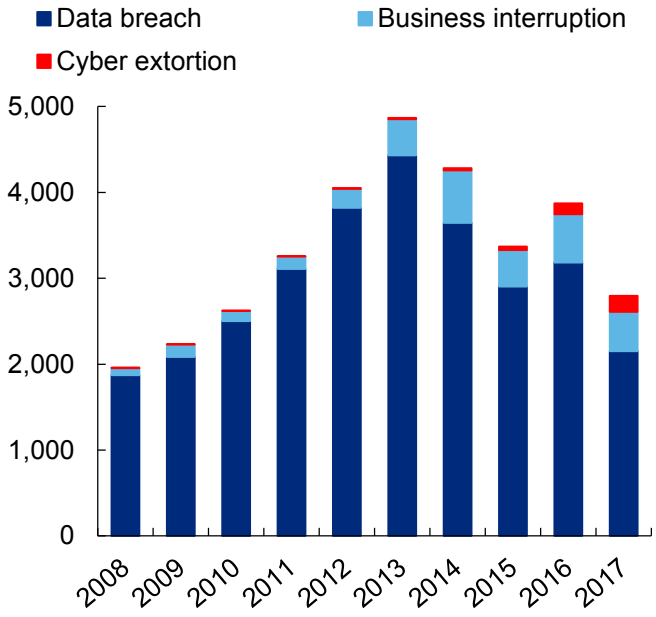
Exhibit 1: Cyber incidents by year and type
(indexed 2008=1.0)



Source: Advisen analysis by Aon Benfield. Data as of 12/27/2017. Note that chart includes any reported cyber incident, whether or not an insurance policy was in place.

Empower Results®

Exhibit 2: Cyber incidents by year and type



Source: Advisen analysis by Aon Benfield. Data as of 12/27/2017.
Note: Reporting lags contribute to the apparent decrease in incidents from 2014 to present.

Breaches remain a considerable concern for both insureds and insurers. While ransomware has dominated headlines, 2017 is reported to be a record year for breaches, according to the Identity Theft Resource Center. Although the Advisen figures do not currently reflect ITRC's assessment, the discovery and reporting of breaches can lag for months. To put this in perspective, in December 2016, there were only 1,600 breaches tracked for the entirety of 2016 – as of December 2017 the 2016 total now stands at over 3,100 breaches.

Aon Benfield Analysis: *Ransomware and wiper accumulation events remain a cause for concern. Ransomware or other extortion events targeting an accumulation point (DNS, cloud, and internet service providers) could impact thousands of insureds at once. Additionally, the way in which these threats continue to manifest suggests that underwriters should consider employee training against phishing and social engineering attacks at least as important as a company's technology suite for cyber defense.*

The exploding value of Bitcoin and other cryptocurrencies continue to play an important role in the proliferation of ransomware and currency-mining malware.

Cryptocurrency values skyrocketed during the fourth quarter, though they have somewhat moderated in early 2018. In particular, Bitcoin saw its value more than triple during the fourth quarter. Nation-states and criminals seeking financial gain are taking notice. In addition to ransomware, in which a ransom is generally demanded in cryptocurrency, cryptocurrency-mining software is on the rise, placing additional strain on antivirus software (and CPUs), thus putting endpoints at increased risk. This is in addition to a rise in targeted attacks on cryptocurrency exchanges and coin wallets.

CoinMiner, a well-known mining malware, now uses *EternalBlue* to propagate – a rather unsurprising development given *EternalBlue's* success in previous campaigns. With other prominent cryptominers like Coinhive infecting endpoints via web compromise and using similar propagation techniques, criminals and nation-states alike are able to easily enslave more machines.

Aon Benfield Analysis: *The impact of crypto-mining remains debatable; to some, it is nothing more than a nuisance. While hijacking a few CPU cycles to mine currency may seem harmless, there have been reports of CPUs being completely overtaken by the malware, rendering the machine useless – an obvious BI scenario. We expect crypto-mining malware infections to increase in direct proportion to the value and viability of cryptocurrencies.*

Industry analysis

Total industry threat alerts in the fourth quarter were down relative to the third quarter according to our analysis, but technology sector alerts are trending up.

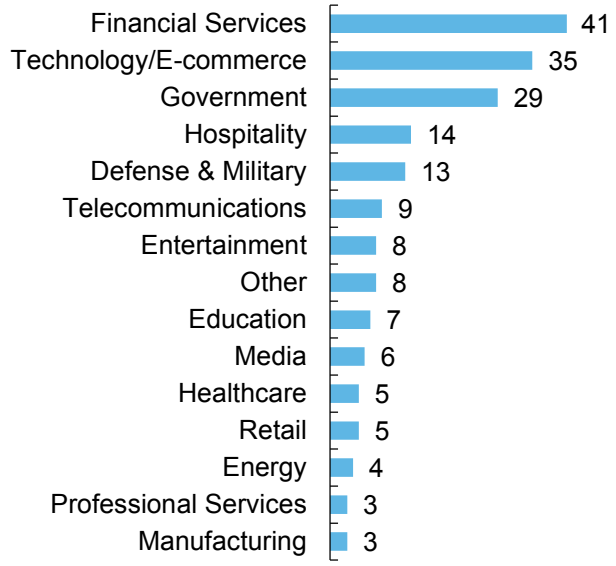
Financial services remained the most frequently targeted industry in the fourth quarter. The well-known banking Trojan *TrickBot* accounted for the vast majority of activity within the sector, continuing a trend from the third quarter.

More noteworthy, though, is that the technology sector surged ahead of government to have the second most alerts in the fourth quarter. How? Banking Trojans such as *Panda Zeus* began to be directed against e-commerce retailers, a key component of the technology industry group (exhibit 3). Bamboo Spider, the actor behind the Trojan, targeted internet retail sites to harvest personal data, credit card numbers, and other sensitive information at far greater numbers during the holiday season.

The expansion of banking Trojans to other industries may be a response to the rise of EMV cards, which includes most chip cards. As cards have become more difficult targets for fraud, criminals are targeting "card-not-present" transactions like e-commerce websites.

North Korean actors continue to target financial institutions and cryptocurrency marketplaces, suggesting the Kim regime continues to seek alternate sources of income. During the fourth quarter, the United States government attributed the WannaCry mass ransomware attack to North Korea, which could continue to inflame cyber-tensions between North Korea and the US. Given the current geopolitical state of affairs, it is reasonable to believe North Korea will continue targeting financial institutions and foment ransomware campaigns.

Exhibit 3: Industry-specific alerts



Source: CrowdStrike, analysis by Aon Benfield Analytics. An alert indicates an imminent incident or event has been observed.

Aon Benfield Analysis: *Criminals continue to adapt their tactics and tools to maximize their financial gain. The fact that in the fourth quarter we saw a noted uptick of Panda Zeus malware targeting online and e-commerce retailers by actors traditionally known for targeting banks drives this point home.*

Cloud downtime

No significant cloud outages were seen in the US in the fourth quarter and average downtimes in North America were lower than in Europe or Asia-Pacific.

Cloud outage scenarios remain a concern, despite little historical precedence of widespread and/or lengthy outages among the major cloud service providers. We did observe cloud outages through January 2018 slightly increase in average downtime per outage in the North American market.

Two of the top seven North American cloud service providers averaged more downtime per outage than the rest of the market. This is a reversal from the third quarter, which saw smaller cloud providers average more downtime.

Microsoft averaged the most of the top seven cloud providers with 27 minutes of downtime per outage (10) and a maximum of just over 42 minutes.

Scheduled maintenance and patching accounted for the majority of downtime during the period observed. Several configuration errors, hardware and software issues were also noted during the quarter.

As a reminder, all the US outages are *extremely short* in duration compared with the typical 8- to 12-hour waiting time insurance deductible.

Asia-Pacific suffered two notable cloud outages in 2017, and cloud-for-ransom attacks emerge.

Sydney, Australia-based Crucial Cloud reportedly suffered a 24-hour outage after a power failure. Unfortunately Crucial Cloud's failure-over power generation systems malfunctioned causing significant damage to some of its hardware. Our initial analysis suggests Crucial Cloud caters to small and medium-sized businesses with several thousand customers affected by this outage. Depending on cyber insurance take-up rates and policy language, this could have been a meaningful aggregation event for Asia-Pacific insurers.

The potential financial gain for disrupting cloud and web services is not lost on criminals and nation-states like North Korea. Earlier in 2017, South Korean web hosting firm Nayana was hit with a Linux-targeting ransomware, which shut down its hosting servers for 5 days. The company agreed to pay over USD1 million in ransom to restore service. Nayana provides hosting services for over 3,400 businesses, potentially resulting in numerous CBI claims if insurance policies were in place.

Exhibit 4: Cloud provider downtime during Q4: Top US providers vs. other regions

Provider	Outages (count)	Avg Downtime (minutes)	Total Downtime (minutes)
North America	227	13	2,868
AWS	2	4	8
Microsoft	10	27	267
Google	-	-	-
IBM	17	12	200
Rackspace	-	-	-
CenturyLink	94	6	546
Oracle	65	19	1,259
All Others	39	15	586
Europe	36	29	1,061
APAC	64	40	2,587

Source: Cloud Harmony, analysis by Aon Benfield Analytics

Aon Benfield Analysis: *In the fourth quarter, observed cloud downtimes and outages exceeded third quarter statistics. Aon Benfield expects cloud outages and associated downtimes to fluctuate based on patching cadences and the occasional software or hardware incident. Nonetheless, the Crucial Cloud outage during the quarter appeared to far exceed typical insurance waiting periods of 8 to 12 hours by a wide margin. Insurance carriers should evaluate their portfolio concentration and total exposed limits with each cloud service provider.*

Emerging story lines

Spectre and Meltdown

The disclosure of the worldwide vulnerabilities *Spectre* and *Meltdown* in January merit special attention. Google's Project Zero identified the vulnerabilities. Both affected hardware (processors) rather than software, and could result in privilege escalation and/or data breach.

Given the severity and ubiquity of both vulnerabilities, major software developers including Apple, Microsoft, and Linux issued software patches soon after Project Zero publicly released its report. However, according to threat intelligence streams, foreign adversaries have attempted to exploit both vulnerabilities since at least December 2017 – with minimal success. In the post-patch environment, the technical sophistication needed to successfully exploit either vulnerability would be extremely high.

Aon Benfield Analysis: *Despite the pervasive nature of Spectre and Meltdown, the issuance of software patches has largely mitigated the threat. However, software patches cannot completely fix hardware vulnerabilities. Highly sophisticated actors could still exploit the vulnerabilities should they decide it worth investing the resources to do so. Therefore, it is important to maintain situational awareness until a new generation of processors are developed and deployed across the world.*

Nation-states continue to dominate the cyber-catastrophe scene.

Months after devastating ransomware campaigns struck Europe, Asia, and parts of North America, these attacks have been largely attributed to nation-states. With the inclusion of the *EternalBlue* exploit, there was always a nation-state component to WannaCry and NotPetya; however, the revelation that North Korea and Russia were the likely culprits reminds the industry that nation-states continue to play a disproportionate role in large-scale aggregation events.

Aon Benfield Analysis: *Unfortunately nation-states – and their loosely affiliated criminal networks – will continue to cause havoc in the digital world. Having insights into the plans and intentions of intelligence services can be extremely difficult to obtain, but invaluable in understanding the threat landscape.*

"Eternal" exploits, and why patching matters

Three lesser-known exploits leaked by the Shadow Brokers – *EternalRomance, EternalSynergy, and EternalChampion* – have been modified by security researchers to exploit all versions of Windows. The original versions of these three exploits did not work on more recent versions of Windows (beyond Windows 7) and thus fell out of favor with threat actors, despite their ability to gain remote access and escalate privileges. Fortunately, Microsoft's patch from March 2017 secures Windows from all of the *Eternal* exploits. Once again, patching cadences matter in determining the security posture and risk level for insureds.

Contact Information

Authors
Jon Laux, FCAS
Head of Cyber Analytics
Aon Benfield
+1 312 381 5370
jonathan.laux@aonbenfield.com

Craig Guiliano, CISSP
Cybersecurity Specialist
Aon Benfield
+1 312 381 1566
craig.guiliano@aonbenfield.com

Aon Benfield Cyber Leadership
Catherine Mulligan
Cyber Practice Group Leader
Aon Benfield
+1 212 441 1018
catherine.mulligan@aonbenfield.com

Luke Foord-Kelcey
Cyber Practice Group Leader
Aon Benfield
+44 (0)20 7086 2067
LFK@aonbenfield.com

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

Disclaimer

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.