Aon Benfield
Cyber

Cyber Threat Insights

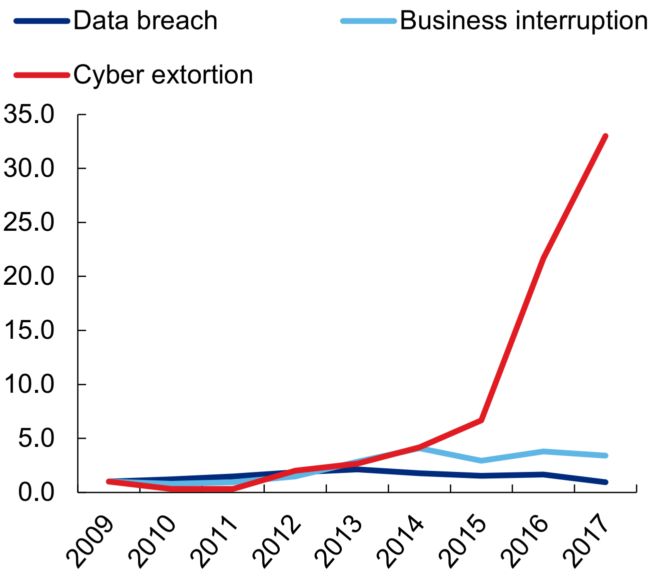
Third Issue, May 2018

Welcome to the third edition of the ***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 end of 2017, cyber extortion rates grew faster than other cyber incidents. But overall, data breaches were the dominant incident type observed.

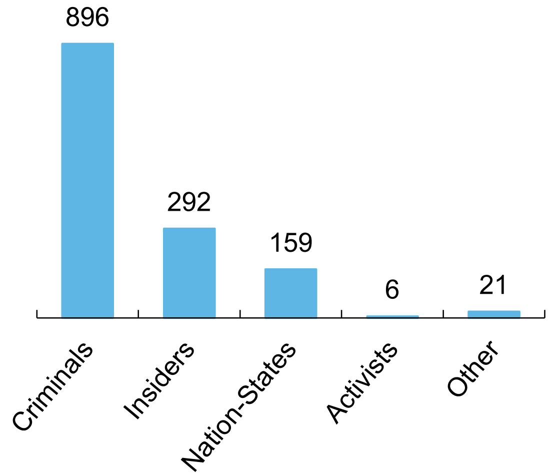
Exhibit 1: Cyber incident rates by year and type (indexed 2009=1.0)



Source: Advisen analysis by Aon Benfield. Data as of 03/27/2018.

Based on Exhibit 1 and our analysis of malware development and deployment, we expect the frequency of business interruption and extortion incidents to continue to increase.

Exhibit 2: Incident count by threat actor (2017)



Source: Verizon *2018 Data Breach Investigations Report;* analysis by Aon Benfield.

Social engineering continues to be threat actors' preferred means of exploitation. Threat intelligence firm Proofpoint contends that email is the preferred attack vector, with banking Trojans and ransomware accounting for 80% of linked malicious traffic.

The infrastructure to conduct attacks remains readily available. During Q1, maliciously registered web domains outnumbered legitimate domain registrations by *20 to 1*, according to Proofpoint. This statistic highlights the broad availability of infrastructure for use by threat actors – and their ability to craft domains similar to legitimate domains to aid in social engineering attempts.

* 2018 figures represent Q1 and experience discovery and reporting delays.

Although not infrastructure per se, Bitcoin and other cryptocurrencies remain highly valued, even as Bitcoin is off its three month high of $12,759, at just over $9,000 at the time of publication. The value of cryptocurrencies has resulted in the proliferation of crypto-mining malware and other incidents that require payment in Bitcoin or other cryptocurrencies. In effect, the value and availability of cryptocurrencies has motivated criminals and nation-states to concentrate their efforts in extortion and crypto-mining, which we will discuss shortly.

During the quarter, the continued commoditization of ransomware assisted criminal upstarts in developing robust ransomware capabilities.

The actors behind the *Globe* (aka *Globe Imposter*) ransomware have advanced the potential of Ransomware as a Service (RaaS). Those interested in designing their own ransomware campaigns can now do so with relatively little skill and limited resources, as these tools are available for sale on Russian underground forums. Although RaaS is not new, the *Globe* ransomware toolkit is highly configurable and comes with a user-friendly interface appealing to a wide cross-section of actors.

Crowdstrike reported that for a nominal fee of approximately $400, nearly any actor can purchase the *Globe* ransomware builder. The *Globe* builder allows customers to customize their malware with basic settings options, bespoke ransom notes, and various encryption algorithms.

Notably, one setting prevents *Globe* from being downloaded onto a computer if the language preferences are Russian, Belorussian, or Ukrainian. This strongly suggests the developers of *Globe* hope to limit the targeting of machines within the borders of these three countries. Although their motive for including this functionality is unknown, it is likely the developers hail from one of the countries listed.

In addition to *Globe,* other ransomware variants have joined the RaaS marketplace, including *Saturn and GandCrab variants.*

Aon Benfield Analysis:
The continued development of RaaS is worrisome, as it significantly lowers the bar for would-be criminals to enter the ransomware business. For around $400, criminals can begin their own ransomware campaign. With ongoing RaaS development and refinement, we expect ransomware attacks to continue trending upward and demand for extortion coverage on cyber insurance policies to increase. Likewise, extortion-related claims are also expected to increase.

Crypto-mining infections have reached fever pitch in the first quarter, hitting as many as 500,000 infections per day.

As reported in Aon Benfield's fourth quarter 2017 *Cyber Threat Insights*, crypto-mining infections continued to escalate through the first quarter of 2018. At one point in March, as many as 500,000 infections were reported per day, according to Microsoft.

In addition, traditional malware – even ransomware – is increasingly including a mineware component. In effect, malware that contains a mineware module will simultaneously infect the victim's computer with crypto-mining malware along with its primary payload, resulting in reduced computing power and, in exceptional circumstances, business interruption.

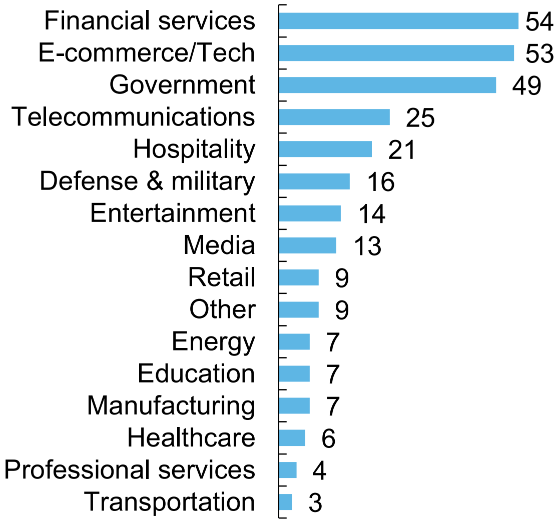
Cryptocurrency exchanges and wallets have also become the *targets* of criminals in cyberspace. Through the quarter, there had been several noticeable thefts of digital currency, including Tokyo-based Coincheck, which lost over $500 million. Due to increases in demand, a growing number of insurers now offer protections for cryptocurrency theft.

***Dridex*, the notorious banking Trojan, continues to evolve, adding new modules through partnerships with various actors.**

After years in the game and millions of dollars stolen, *Dridex* remains a highly sophisticated, continuously-evolving malware suite with which financial institutions must contend. *Dridex* now offers point of sale skimmers (POS) and ransomware modules, in addition to its traditional tools for stealing banking credentials and other personally identifiable information (PII), according to Crowdstrike. These partnerships make a piece of sophisticated malware like *Dridex* even more dangerous. *Dridex* was observed targeting e-commerce, retail, and hospitality during the quarter.

Aon Benfield Analysis: *The evolution of malware can be directly attributed to market conditions – and criminals are tweaking their wares to take advantage. Regardless, criminals still largely rely on automation to identify weakness in a company's internet-facing hardware and software. Underwriters that can readily identify these "low hanging fruit" via external assessments can reduce their exposure.*

Exhibit 3: Industry-specific threat alerts



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

Industry analysis

As with previous quarters, financial services remained the most frequently targeted industry. As has been reported in past issues of the *CTI*, sophisticated banking Trojans continue to target online banking and, to a lesser extent, other industries such as e-commerce.

Despite the March arrest of the alleged leader of the Carbanak Group – a sophisticated criminal group responsible for attacking the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system – attacks against the financial services industry remain high. In addition, state-sponsored actors like the North Korean-affiliated Lazarus Group or "Hidden Cobra" increased their targeting of financial institutions, cryptocurrency exchanges, and wallets – as seen in recent reporting on Operation GhostSecret.

Healthcare remains squarely in the crosshairs of criminals despite the relatively small number of alerts issued for the industry.

Despite the relatively few alerts issued for the healthcare industry, it has been disproportionally affected by ransomware and other attacks. Sophisticated criminal groups like the *Samas* ransomware group (aka *SamSam*, *Boss Spider*) have specifically targeted healthcare. The most recent ransomware attacks against government institutions – the city of Atlanta, Georgia and Colorado Department of Transportation – were also attributed to *Samas*.

Aon Benfield Analysis: *Financial institutions remain the most targeted industry, but usually deploy robust defenses. On the other hand, criminals seek out healthcare and government institutions because of their less-than-adequate defenses. Underwriters should consider passing on potential insureds with glaring misconfigurations or outdated encryption, which indicate poor security practices across the board.*

Cloud downtime

Cloud downtime during the quarter remained within expected limits. The data for Q1 reflects trends identified during Q4 of 2017 – large providers experience less downtime when compared to mid-market providers.

The top cloud service providers experienced no downtime during the quarter. Amazon Web Services* (AWS), Microsoft, Google, IBM, and Rackspace experienced zero outages. Smaller and regional providers suffered longer downtimes, when compared to their larger (by market share) peers.

*Despite AWS' 100% uptime record for the quarter, AWS Direct Connect customers utilizing AWS-US-East Region experienced a notable outage on March 2nd. Amazon blamed the outage on the "loss of power to one of AWS's redundant interconnection points." It is still unclear if AWS or its partners were at fault, but it was reported that over 200 businesses were affected for approximately four hours.

Exhibit 4: Cloud provider downtime during Q1: Top US providers vs. other regions

Provider	Outages (count)	Avg Downtime (minutes)	Total Downtime (minutes)
North America	285	64	18,342
AWS	-	-	-
Microsoft	-	-	-
Google	-	-	-
IBM	-	-	-
Rackspace	-	-	-
CenturyLink	68	9	589
All Others	217	82	17,752
Europe	36	29	1,061
APAC	64	40	2,587

Source: Cloud Harmony, analysis by Aon Benfield Analytics

Aon Benfield Analysis: *In the first quarter of 2018, observed cloud downtimes were minimal relative to the typical 8- to 12-hour insurance waiting periods. The most popular cloud providers logged much less downtime than Q3 – a trend we attributed to less-than-routine patching related to the Spectre and Meltdown vulnerabilities. We expect continued volatility with mid-market providers and underwriters should limit their exposure accordingly. Aon Benfield can help identify overexposure to specific cloud and other internet service providers.*

Emerging story lines

For the first time on record, the US and UK governments issued a public warning of Russian attempts to target networking hardware and software – specifically routers. The announcement came in the aftermath of a particularly divisive week – Russia and multiple NATO countries expelled a record number of each other's diplomats; the US government struck Syria, an ally of Russia, after an alleged chemical weapons attack; and Russia and western allies exchanged heated accusations at the United Nations.

Although attacking routers is not a new tactic – and Russian-linked actors have been noted to collect information on networks in the past – it is likely this type of activity will increase given the current state of Russia's relationships with western nations.

Aon Benfield Analysis: *Given the current geopolitical tensions between Russia and the West, it is likely that Russia will increase its "hybrid warfare" activity, to include cyber espionage targeting critical infrastructure and government institutions. In recent months, Russia has been implicated in a number of high-profile cyber reconnaissance activities targeting critical infrastructure in the US by various Russian actors. We expect these activities to continue, and potentially escalate if tensions continue to rise.*

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

This newsletter is made available for informational purposes and is not intended to be a substitute for professional or legal advice. No attorney client relationship is formed or implied between you and the authors(s) or Aon Benfield.

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