Tackling the DDoS Threat to Banking in 2014

DDoS gets bigger, smarter, and more blended

Reference Code: EI003-000020
Publication Date: 27 Jan 2014
Author: Rik Turner

SUMMARY

Catalyst

The distributed denial of service (DDoS) threat landscape against financial institutions has evolved over the past year, with politically motivated "hacktivists" emerging as a new source of attacks alongside the more traditional hackers seeking financial gain. The hacktivists use massive DDoS attacks and have targeted a number of major banks, particularly in the US. Meanwhile, a more recent trend has seen such DDoS attacks being used to detract attention from more conventional, financially motivated exploits, while still others are using smaller but smarter DDoS to avoid detection. Ovum considers banks' options in the current environment.

Ovum view

DDoS attacks have undergone significant evolution over the past year. On the one hand they have grown larger, even while their average individual duration has actually decreased. Attacks as widespread as those mounted in Operation Ababil – a coordinated series of DDoS attacks started in September 2012 against US financial institutions and entities such as the New York Stock Exchange – are still the outliers rather than the norm, with average traffic sizes less than a 20th of what Ababil was throwing at banks' websites at its height, and the sustained nature of those attacks was quite out of character with what most DDoS looks like.

Still, while something of an anomaly, Ababil points in one direction that DDoS can go, given the availability of ever larger and cheaper botnets. Another is to harness more sophisticated technologies, such as headless browsers, that enable relatively small attacks of a shorter duration to go undetected and potentially wreak their own kind of havoc on a bank's website.

The other trend Ovum sees is the blending of DDoS with other forms of exploit, often to throw banks off the track of, say, an account hijack so that the criminals can enjoy more time to transfer funds and remove traces of their activities before the institution has time to contact a counterparty bank and back out a transaction, for instance.

All these developments point to the need for a multilayered approach to DDoS mitigation, with part of a bank's infrastructure addressing the more sophisticated, finely targeted attacks with filtering, while another part can address the blunt instrument of a volumetric attack by absorption tactics. Over time, a single vendor may emerge that can address both requirements, but for the time being, Ovum believes banks will need to mix and match solutions, possibly opting to put some on premise while others can be delivered as a service from the cloud. DOS absorption seems inherently more suited to a service, given the capex involved in adding bandwidth and infrastructure on premise; filtering/scrubbing can certainly still be done by an on-premise appliance, though here too we see the rise of specialized service providers such as Incapsula and DOSarrest. And of course, the recent acquisition of the most established scrubbing service provider Prolexic by the leading advocate of DOS absorption as a service, Akamai, suggests that the entire gamut of DOS mitigation services will shortly be available from a single source.

Key messages

- Political DDoS is fundamentally different from "traditional" hacking.
- DDoS attacks are becoming more variegated.
- The majority of banking institutions plan changes in IT security in 2014.
- Cloud-based security will help banks mitigate DDoS attacks.
- Combining filtering and absorption techniques is recommended.

POLITICAL DDOS IS FUNDAMENTALLY DIFFERENT

The threat landscape is continually evolving

The world of information security is one of continual change, as technological development has enabled new ways of working with information but also new ways of stealing, defacing, or otherwise compromising it. The development of the Internet, its wholesale adoption by companies engaging in e-commerce, and now its extension into areas such as healthcare and government have all been incentives for new types of security exploits, and indeed the hackers themselves have evolved.

In the early days of the Internet, the majority of hackers were computer-savvy individuals in Western countries seeking notoriety, albeit for the aliases they used, as portrayed in the 1995 Hollywood movie *Hackers,* whose lead character uses the moniker "Zero Cool" at one stage in his career. For over a decade now, they have been replaced by commercially minded groups seeking some form of financial advantage, whether by extracting money from a bank account, spending on someone else's credit card, or stealing intellectual property for their own use or to resell to other interested parties.

This scenario has dominated the world of cyber security since the turn of the millennium and is clearly not going away. That said, though, the past couple of years have witnessed the rise of two new phenomena.

First, the risk of the insider threat, though always present, has come more sharply into focus as a result of the WikiLeaks scandal surrounding leaks by US soldier Bradley Manning and, more recently, of the

Edward Snowden case and its revelations of US National Security Agency snooping on individuals around the world.

Second, since 2012 we have seen the emergence of politically motivated hacking, or hacktivism, with financial institutions as a particular target for such activity.

QCF hacktivism emerged in September 2012

Hacktivism has been around for at least a decade, with the Anonymous group emerging from posts on the /b/ board of the 4chan imageboard as long ago as 2003 and coalescing around hacktivist behavior circa 2008. However, the advent of Operation Ababil really raised the profile of such activity.

The group claiming responsibility for Ababil is the Cyber Fighters of Izz ad-Din al-Qassam, or the al-Qassam Cyber Fighters (QCF) for short. Their ideology is overtly anti-Western, anti-capitalist, and anti-American, and their objective has been to cause high-profile operational problems to US financial institutions in order to provoke the suppression of a video critical of Islam posted on YouTube by conservative Christian preacher Terry Jones. Ababil has so far had four separate phases of attacks, the first unleashed in September 2012 and the fourth in July 2013.

While infosecurity industry professionals have differed in their opinion as to the sophistication of the attacks, their sheer size is undeniable: at their height, as much as 120 gigabits per second (Gbps) of traffic, all of it encrypted, was being launched at the targeted websites. This compares with the average size of normal DDoS attacks of just 2Gbps and has led several industry pundits to speculate that QCF is state-sponsored rather than a private group of malcontents, with the favorite suspected backer being the government of Iran. There have also been allegations that Anonymous has helped the QCF, though no convincing evidence of this has yet emerged.

Post-attack evidence showed that QCF was refining its strategies as it went along: in the latter phases of Ababil, they adopted a strategy of rotating the attack between many servers, so that while the overall volume was 30–60Gbps for most attacks, the sources of the traffic were varied, allowing them to attack multiple targets simultaneously.

Another difference between Ababil and conventional DDoS attacks was its persistence. Most DDoS attacks are relatively short, lasting a few hours at most, whereas Ababil was relentless in attacking certain targets for days at a time. Like the sheer volumes of traffic it threw at websites, this points to the fact that the QCF had considerable firepower and further fueled speculation about state sponsorship of its activities.

Phase 4 of Ababil, in July 2013, was notable for its weakness. The three earlier rounds had targeted almost 50 US banks, ranging from household names such as JPMorgan Chase and Bank of America to smaller institutions such as PNC Financial Services and Zion's Bank. By contrast, Phase 4 attacked only two institutions (though admittedly, one of them was JPMorgan Chase again), and then only for a couple of days in total.

It would be premature, and perhaps even foolhardy, to declare the end of Ababil, or indeed the demise of the QCF. In August 2013 the FBI said arrests it had made of six leading hackers had essentially neutralized Anonymous, but 24 hours later an Anonymous affiliate on Twitter called OpLastResort retaliated by releasing personal information pertaining to some 23,000 employees of the US Federal Reserve.

Thieves are surreptitious, while hacktivists court publicity

There is a fundamental difference here between financially motivated cybercrime and hacktivism, namely that perpetrators of the former have a vested interest in remaining below the radar, since they are stealing money or intellectual property and thus actively seek to remain undetected, whereas at the end of Phase 1 of Ababil, the QCF actually announced that they were now available for conversations via email with the Western press. Of course, the individuals involved still want to remain anonymous, but they are publicizing a cause rather than seeking immediate and illicit financial gain.

For financial institutions, however, the impact of either type of hack is potentially as damaging. While a robbery from an individual account can possibly be kept relatively quiet, with only the client themselves and a financial authority involved, a disgruntled customer may take legal action or a regulator may publish information on the hack if it deems it to be in the public good. On the other hand, a "political" hack such as Ababil may be short-lived, but it is by definition a high-profile action designed to spread fear and dread among bank customers.

DDOS BECOMES MORE VARIEGATED

The cloud makes large-scale DDoS cheaper and easier

As already mentioned, the sheer size of the Ababil attacks has heightened the suspicion that they are state-sponsored operations. If so, they would only be the latest and most high-profile example of alleged state-backed cyber terrorism, dating back at least to 2007 when Estonia's foreign minister openly accused the Kremlin of being involved in a series of coordinated attacks Estonian government and financial websites carried out from IP addresses located predominantly in Russia.

In reality such volumetric DDoS attacks are still very much in the minority. Data from security firm Arbor Networks shows that DDoS attacks in general became more powerful in 2013 while their duration declined. The average DDoS attack size through October 2013 was 2.64Gbps, far below the intensity of the Ababil operation but still an increase of 78% from 2012, while some 87% of attacks lasted less than one hour.

However, the economics of large-scale DDoS are changing. The QCF uses a botnet, or network of controlled machines, called Brobot, which it appears to build and control itself. However, cloud economics are creeping into every area of IT at the moment, and since botnets have long been available as a service, there is every possibility that a vast botnet, capable of delivering the kinds of traffic volumes that Ababil could command, can and will become available on demand and as a service, enabling cybercriminals to adopt massive DDoS as a tactic for their own ends.

Headless browsers have made narrowband DDoS attacks smarter

While volumetric DDoS is facilitated by the availability of botnets for hire, another technological development, headless browsers, has made it easy for targeted DDoS attacks to get smarter.

A headless browser is a web browser without a graphical user interface, which means that it accesses web pages without showing them to a human being. Instead, headless browsers are used legitimately to provide the content of web pages to other programs. For instance, Google has said that using headless browsers is a way to enable its search engine to cope with AJAX code. App developers commonly use headless browsers to test their code and simulate user browsing.

However, this also opens up possibilities for DDoS attackers. In October 2013, for instance, DDoS mitigation service provider Incapsula said one of its customers, a trading platform whose identity it did not reveal, had been subjected to a 150-hour DDoS attack using 861 variants of the headless browser technology Phantom JS to simulate legitimate user browsing behavior and thus avoid detection.

DDoS now becomes part of a new blended threat arsenal

There are already signs that DDoS has moved on from its use by the hacktivists. Whether or not Ababil is finished, it is clear that DDoS has moved into the mainstream of security exploits and is now being blended in with other types of attack by cybercriminals.

Some pundits are referring to DDoS as a distraction mechanism in such blended attacks, but in fact the most serious impact, in the context of financial services institutions, is achieved when it is used to delay a bank's response. For instance, if a customer's account has been hacked and funds transferred to a third party, a DDoS attack can then be launched to flood the bank's network and keep its IT department busy, giving the criminals more time to make a "cyber getaway," transferring the funds to still other accounts and covering their tracks.

We have yet to see a large-scale DDoS attack along the lines of what Ababil could muster used as part of a blended attack with financial motives. Ovum believes it is only a matter of time until we do, however, given the changing economics of DDoS and the availability of ever more and cheaper botnets.

Smarter authentication has a role to play against the new DDoS

While absorption and filtering/scrubbing are undoubtedly the main approaches to combatting DDoS, other information security systems also have a role to play. An example is authentication technology, where leading vendor RSA has added functionality into the latest version of its Adaptive Authentication platform specifically to address such exploits. It can now detect, for instance, whether information is being input without mouse or key clicks (an indication that it is coming from a non-human source) and then raise the risk score of the transaction and step up authentication requirements, for instance by triggering a call to the user's mobile phone. It can also detect whether a user is coming in from a proxy server by pinging the external host and seeing how long the response takes, then comparing its data to see whether that user commonly comes in that way or the situation is anomalous.

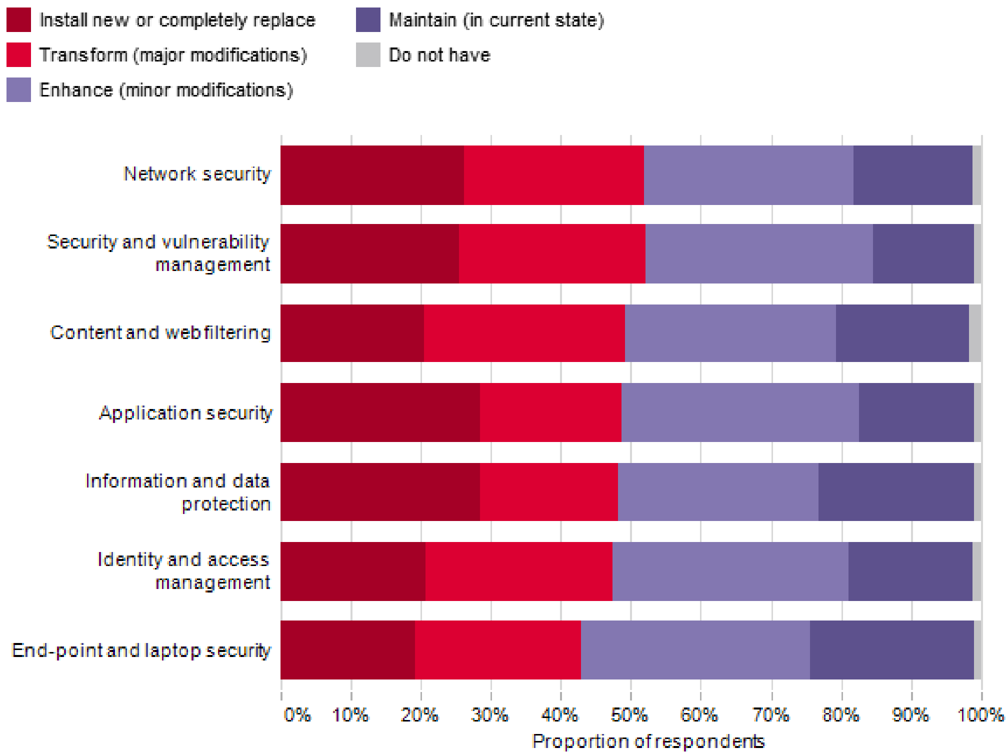
RSA further stepped up its capabilities in this area with its late-2012 acquisition of Silver Tail Systems, which brought it a Web threat detection platform. Silver Tail sits on a SPAN port in a network and ingests all incoming HTTP and HTTPS requests, upon which it creates a baseline of normal behavior that enables it to pick up anomalous activity suggesting man-in-the-middle, man-in-the-browser, and Layer-7 DDoS attacks, as well as vulnerability probing and HTML injection. The plan is to integrate Silver Tail (soon to be rebranded RSA Web Threat Detection) with the Adaptive Authentication platform to further enhance the latter's ability to combat DDoS and other forms of Web exploits.

THE FINANCIAL SECTOR IS INVESTING IN SECURITY IN 2014

The majority of financial services firms plan changes in IT security

Ovum's annual ICT Enterprise Insights survey for 2013 spoke to 948 financial service institutions across the globe, drawing on sources from retail banking, the financial markets, and the insurance industry to find out about their IT spending plans for the coming year. Across seven different areas ranging from network to endpoint security, the consistent message was that only a relatively small percentage of institutions plan to maintain their current security infrastructure unchanged through the end of 2014. The majority told Ovum that they would either install new or completely replace what they had in place when the survey was carried out (3Q13), undertake major modifications to their existing infrastructure, or at the very least, significantly enhance it.

Figure 1: Financial services firms' IT security investment plans



Copyright: Ovum

Sample size: 948
Question: What are your investment plans for the above during the next 18 months?
Countries: All. Vertical: All. Sub-vertical:Buy side, Consumer banking and 3 more. Enterprise size: All.

Source: Ovum ICT Enterprise Insights

Under the heading of network security, just 16% of respondents said they planned to leave things as they currently are, while almost 49% said they anticipated major modifications or a complete replacement. Meanwhile in security and vulnerability management (the proactive assessment of vulnerabilities so as to address them before any exploits), 52% planned a major upgrade or replacement of existing infrastructure.

CLOUD CAN HELP BANKS MITIGATE DDOS ATTACKS

Responses to DDoS fall into four categories

The number and size of DDoS attacks is growing, even if sustained, large-volume ones like Ababil are still the exception rather than the norm. The options banks have for responding to DDoS exploits fall broadly into four categories.

1. Deploy more network and infrastructure

One way of addressing the floods of incoming traffic that DDoS generates in order to hamper the functioning of a company's website is simply to add a lot more network bandwidth and web servers in the hope that this expanded infrastructure will be able to cope. This approach works up to a point but is of course expensive, and it can come under severe pressure when the attack is volumetric.

2. Use a content delivery network (CDN) to absorb the attack

Instead of adding its own network capacity as in option 1, a bank can opt to use the services of a CDN for the same purpose. The most proactive of the commercial CDNs in terms of responding to the challenge of DDoS has been Akamai, which offers its Kona Site Defender service precisely to soak up additional traffic from DDoS attacks and thus mitigate their impact. Akamai has tens of thousands of servers deployed worldwide in its CDN, such that even massive attacks like Ababil have been addressed for clients in the financial sector. Not surprisingly, Akamai makes much of its capabilities in this context in its marketing of the Kona service.

3. Deploy an on-premise filtering appliance

Banks can opt to deploy on-premise appliances to filter out DDoS traffic, which along with option 1 is the most traditional approach to this problem. The challenge here is that, as attacks grow in volume, institutions could end up spending increasing amounts on such on-premise infrastructure and, worse still, having to manage an entire estate of dedicated filtering appliances.

4. Use a cloud-based filtering service aka a scrubber

The other alternative for filtering is to do it in the cloud, in which case a bank will use the services of a third-party filtering provider, also known as a scrubber, to whom all inbound web traffic is routed prior to hitting the bank's own servers, with the scrubber taking out all the malicious parts and forwarding only the legitimate traffic to its customer's website.

Each approach has pros and cons

Of course, none of these approaches is perfect. Options 1 and 2 are both absorption strategies, and while they can certainly mitigate volumetric attacks they are prone to forward to a bank's actual web servers traffic coming from a headless browser and thus imitating real users' behavior, since they do not inspect the inbound traffic.

Conversely, options 3 and 4 are both based on filtering, which is clearly more appropriate for addressing attacks based on headless browser–generated traffic but may struggle with a volumetric attack, as both on-premise and third-party scrubber infrastructure will almost certainly be more limited than anything a CDN like Akamai can throw at such a problem.

COMBINING FILTERING AND ABSORPTION IS RECOMMENDED

Given the dichotomy of DDoS attack types, a multilayered approach is clearly the most advisable, with one layer dealing with volumetric threats while another addresses the more narrowband attacks that are now harnessing new obfuscation techniques such as headless browsers. Whether a bank prefers to have all its mitigation capabilities entirely on premise, in the cloud, or a mixture of the two will be dictated at least in part by its risk posture. Indeed, the debate between the two approaches is reminiscent of that which raged a decade or more ago over where best to place email filtering facilities.

By and large, that debate was won by managed service providers, and Ovum's suspicion is that the same will ultimately be true for DDoS mitigation, particularly if volumetric attacks start to proliferate and became a larger part of the overall DDoS landscape.

Either way, it is clear that a mixture of absorption and scrubbing is required, tacit recognition of which came from Akamai itself at the end of 2013, when it acquired the most established name in the scrubber community, namely Prolexic.

RECOMMENDATIONS

Recommendations for enterprises

Be prepared to mix solutions from different vendors

It would be nice if a single vendor could offer comprehensive protection against both the volumetric type of DDoS attack we have seen in Ababil and more targeted attacks that use headless browser technology to avoid detection. While Akamai's acquisition of Prolexic holds the promise that such a provider may eventually emerge, it is too early to say how successful a Kona+Prolexic service will actually be, and work will likely be needed to integrate the two activities.

Don't discount on-premise appliances out of hand

While the cloud-based service providers are clearly an attractive proposition for keeping DDoS traffic entirely off your premises, there may be some particular type of detection routine, or a particular type of analysis that your organization wants to carry out, that is just too specialized or custom to be available from a cloud-based provider with multiple customers.

Recommendations for vendors

Whether on-premise or cloud-based, acknowledge your offering's limitations

Given the current state of development of DDoS mitigation approaches and the technical advances that the attackers themselves are going through, Ovum considers it the best policy for vendors to admit that what they are offering is only part of an overall solution and to advocate a multilayered strategy to their customers. While this may not be, a priori, what the customers want to hear, it is better to deal with their irritation up front and explain the reasons for your honesty than to sell them what they hope will be the definitive solution and then deal with their frustration after a different type of DDoS attack has hit them and circumvented your product/service.

Seek alliances with mitigation vendors in the other camp

Akamai's acquisition of Prolexic points to how the industry will evolve, with further alliances between DDoS absorption and scrubbing vendors going forward. Whichever camp you are in, seek alliances with firms in the other camp for a combined offering that can address the challenges of the different types of DDoS attack now emerging.

Alternative views

DDoS exploits will fizzle out over the coming years as attackers move to alternative means of hitting their targets. As such, mitigation technology will become irrelevant, as nobody is any longer mounting significant attacks.

APPENDIX

Further reading

SWOT Assessment: F5 Networks BIG-IP Platform, V11.4, IT017-004229 (December 2013)

SWOT Assessment: Arbor Networks Peakflow and Pravail, IT017-004216 (November 2013)

SWOT Assessment: Incapsula DDoS Protection, IT017-004215 (November 2013)

SWOT Assessment: Akamai, Kona Site Defender, IT017-004197 (September 2013)

SWOT Assessment: Corero Network Security, DDS-5500, Release 6.80, IT017-004171 (July 2013)

Author

Rik Turner, Senior Analyst, Financial Services Technology

rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Disclaimer

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions, and recommendations that Ovum delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such Ovum can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect.