Mitigating the Risk of Distributed Denial-of-Service (DDoS) Attacks

Jonathan Foxx *

On Tuesday, April 1, 2014, Ellie Mae's systems were compromised by a Distributed Denial-of-Service (DDoS) attack. Resources known to be affected were all Encompass services, including Encompass Docs Solution™, Electronic Document Management ("eFolder"), Encompass Product and Pricing Service™, Encompass Compliance Service™, and Ellie Mae Network Services.[1]

Ellie Mae itself proactively published a Press Release on April 1st, announcing that "recent outages [that] have made Ellie Mae's Encompass services unavailable to users." And further stating that it "has detected unusually high demand for services consistent with an external malicious attack characteristic of a distributed denial of service (DDoS)."[2]

As reported by Bloomberg at the time, the system failure "prevented some mortgages from closing." One client complained that "our business is at a standstill."[3]

For our own clients, we sought to know how Ellie Mae was challenging this attack and also we monitored its status page.[4]

By Wednesday, April 2nd, Ellie Mae's focused and deliberative handling of this matter was bringing the overall problem to the stage of being resolved. The completion was met with a statement by Sig Anderman, Ellie Mae's CEO, with a statement affirming that, "as of 2:15 p.m. PT, we verified that Encompass Homepage login and load times have returned to normal."[5]

*** Author: Jonathan Foxx, President & Managing Director, Lenders Compliance Group**
Publication: National Mortgage Professional Magazine – April 2014

As it happens, and quite coincidentally, on April 2nd the Federal Financial Institutions Examination Council ("FFIEC") issued a statement to notify institutions of "the risks associated with the continued distributed denial of service (DDoS) attacks on public-facing Web sites and the steps institutions are expected to take to address the risks posed by such attacks."[6]

I well remember meeting a compliance officer of a relatively large bank at his office. He asked me to step around his desk and take a look at his screen. I was astonished to see thousands and thousands of green coded lines scrolling on the screen. I asked him what was going on, and he told me that the bank's systems were under attack and these were the unending attempts to penetrate their systems. I had never seen anything like it!

Let's take a brief trip into this area of Internet madness that IT professionals deal with daily.

Since 2012, there has been an increasing number of DDoS attacks launched against financial institutions by politically motivated groups, so says FFIEC. However, we also know that DDoS attacks have come from foreign country proxies, mafia-type criminals, and sundry other nefarious individuals and organizations hell bent on disrupting financial institutions. DDoS attacks serve as a diversionary tactic by criminals attempting to commit fraud using stolen customer or bank employee credentials to initiate fraudulent wire or automated clearinghouse transfers.

These DDoS attacks have increased in sophistication and intensity, almost to the point that they are commonplace. The attacks cause slow website response times, intermittently prevent customers from accessing institutions' public websites, and adversely affect back office operations.

Thus, many financial institutions are considerably at risk to information security failures and even entire system implosions. Financial institutions of all sizes that experience DDoS attacks may face a variety of risks, including operational risks and reputation risks. And if the attack is coupled with attempted fraud, a financial institution may also experience fraud losses as well as liquidity and capital risks.

FFIEC suggests that financial institutions should address DDoS readiness as part of ongoing information security and incident response plans. Through FFIEC, such readiness has been proposed by the Board of Governors of the Federal Reserve System (FRS), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), Consumer Financial Protection Bureau (CFPB), and the State Liaison Committee. Many states now mandate adopting an Information Security Plan that contains many elements of readiness, incident response, and certain risk mitigation procedures.

There are actions a financial institution's management would be wise to take to mitigate the risks associated with DDoS attacks, given the company's size, complexity and risk profile. Any plan to mitigate such risks should include the following elements:[7]

1. Maintain an ongoing program to assess information security risk that identifies, prioritizes, and assesses the risk to critical systems, including threats to external websites and online accounts;

2. Monitor Internet traffic to the institution's website to detect attacks;

3. Activate incident response plans and notify service providers, including Internet Service Providers (ISPs), as appropriate, if the institution suspects that a DDoS attack is occurring. Response plans should include appropriate communication strategies with customers concerning the safety of their accounts;

4. Ensure sufficient staffing for the duration of the DDoS attack and consider hiring pre-contracted third-party services, as appropriate, that can assist in managing the Internet-based traffic flow. Identify how the institution's ISP can assist in responding to and mitigating an attack;

5. Consider sharing information with organizations, such as the Financial Services Information Sharing and Analysis Center[8] and law enforcement because attacks can change rapidly and sharing the information can help institutions to identify and mitigate new threats and tactics; and

6. Evaluate any gaps in the institution's response following attacks and in its ongoing risk assessments, and adjust risk management controls accordingly.

I strongly recommend that the management of a financial institution meet regularly with the Chief Information Officer ("CIO") or, in lieu of a CIO, the IT professional who is in charge of maintaining the institution's systems. Furthermore, every CIO and IT professional should be fully versed in the requirements set forth in FFIEC's booklets, *Information Technology Handbook on Business Continuity Planning*[9] and *Information Security*.[10]

Another resource is the DDoS Quick Guide, dated January 29, 2014, published by the Department of Homeland Security's National Cybersecurity and Communications Integration Center.[11] This guide provides useful information on attack possibilities and traffic types. It should be shared with an institution's IT department and the institution's online banking and website service providers, if applicable.

Finally, there are the publications such as National Institute of Standards and Technology's[12] "Special Publication 800-61," the *Computer Security Incident Handling Guide*,[13] which offers specific instructions for IT staff members to help implement incident response plans. Also helpful are the reference materials from the OCC, *Distributed Denial of Service Attacks and Customer Account Fraud*,[14] the NCUA, *Mitigating Distributed Denial-of-Service Attacks*,[15] and the "Security

Tip (ST04-015)" from the United States Computer Emergency Readiness Team (US-CERT),[16] *Understanding Denial-of-Service Attacks*.[17]

---

[1] Update – Encompass Incident Alert (4/3/14): http://www.elliemae.com/network-status
[2] *Ellie Mae Reports on System Outages*, "Outage Consistent with External Malicious Attack, No Evidence of Data Breach," Press Release, April 1, 2014
[3] Bloomberg News, *Ellie Mae Technical Breakdown Prevents Mortgages From Closing*, Heather Perlberg and Kathleen M. Howley (Apr 1, 2014 1:36 PM ET): http://www.bloomberg.com/news/2014-04-01/ellie-mae-technical-breakdown-prevents-mortgages-from-closing.html
[4] Ellie Mae's status page (4/3/14): http://www.elliemae.com/network-status
[5] Anderman, Sig, *Encompass Incident Update from Ellie Mae*, Encompass Incident Update, Ellie Mae, April 1, 2014: http://www.elliemae.com/encompass-incident-update
[6] Joint Statement, *Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources*, FFIEC, FIL-11-2014, http://www.fdic.gov/news/news/financial/2014/fil14011.html
[7] Idem
[8] Financial Services Information Sharing and Analysis Center (FS-ISAC): https://www.fsisac.com
[9] *Information Technology Handbook on Business Continuity Planning*: http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx
[10] *Information Security*: http://ithandbook.ffiec.gov/it-booklets/information-security.aspx
[11] National Cybersecurity and Communications Integration Center (NCCIC): https://www.dhs.gov/about-national-cybersecurity-communications-integration-center
[12] National Institute of Standards and Technology (NIST): http://www.nist.gov
[13] Computer Security Incident Handling Guide: http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf
[14] Distributed Denial of Service Attacks and Customer Account Fraud: http://www.occ.gov/news-issuances/alerts/2012/alert-2012-16.html
[15] Mitigating Distributed Denial-of-Service Attacks: http://www.ncua.gov/Resources/Pages/RSK2013-01.aspx
[16] United States Computer Emergency Readiness Team (US-CERT): http://www.us-cert.gov
[17] Understanding Denial-of-Service Attacks: http://www.us-cert.gov/ncas/tips/ST04-015