Available online at www.postmodernopenings.com

e-ISSN: 2069–9387; ISSN–L: 2068–0236

Postmodern Openings

2016, Volume 7, Issue 1, June, pp. 21-34

Ongoing Threats to Emerging Financial Entities

Bryce Alexander LYNCH

DOI: http://dx.doi.org/10.18662/po/2016.0701.02

Covered in:
EBSCO, ERIH PLUS, CEEOL, Ulrich Pro Quest, Cabell, Index Copernicus, Ideas RePeC, EconPapers, Socionet, Journalseek, Scipio

How to cite: Lynch, B. A. (2016). Ongoing Threats to Emerging Financial Entities. *Postmodern Openings*, *7*(1), 21-34. Doi: http://dx.doi.org/10.18662/po/2016.0701.02

DOI: 10.18662/po/2016.0701.02

Ongoing Threats to Emerging Financial Entities

Bryce Alexander LYNCH[1]

Abstract

In the twenty-first century the pace of technological advancement shows no signs of stopping. Old technologies are being discarded as obsolete or are transformed in ways that nobody could have foreseen even a half-decade ago. Along with these radical changes come vulnerabilities and threats to infrastructure, including informational and financial which must be considered and protected. This is not to say that basic security measures must continue to be neglected in favor of rapid development and deployment to provide a Minimum Viable Product to customers; basic security protocols become all the more important under these circumstances. Improving faster are attacks against the new infrastructure; technique and technology tend to change along generally accepted sets of rules while attackers follow no rules or guidelines. This fundamental asymmetry leaves defenders at a distinct advantage in several ways, including ethical concerns ("There are some lines we will not cross" versus "By any means necessary"), monetary considerations ("Return on investment" versus "The resources aren't ours to begin with, so who cares") and pragmatism ("We exist to make money to improve shareholder value" versus "Because it's there"). That said, measurable, repeatable, and effective countermeasures exist which can be deployed on an enterprise-wide basis to help level the playing field by deterring attackers. This paper will discuss these threats along with active and passive countermeasures for same.

Keywords:

Information security, emerging economies, finance, intelligence, threats, modus operandi, countermeasures, industrial espionage.

[1] Information Security, Ripple, Bay Area, California, drwho@virtadpt.net.

Lynch, B. A. (2016). Ongoing Threats to Emerging Financial Entities. Postmodern Openings, 7(1), 21-34. Doi: http://dx.doi.org/10.18662/po/2016.0701.02

1. Introduction

The Internet has caused revolution after revolution in multiple fields since the late 1990's, such as organization of social groups, commerce, law enforcement, banking, software development, and currency remittance. In the early twenty-first century each successive wave of changes occurred faster and faster, changing things near and far before people could fully appreciate the scope of those changes to their everyday lives or assess the potential impact for good or for ill. Unfortunately but inevitably change to any kind of infrastructure brings new vulnerabilities which are not fully characterized. For example, few people suspected that connecting industrial control systems to the Internet without incorporating standard security countermeasures (firewalls, et al) would leave power substations completely vulnerable because these control systems were never designed with security in mind. The same can be said of the infrastructures of emerging financial institutions, such as cryptocurrency gateways and international remittance companies. At this time there are three major threats to these business fields: The companies themselves, unscrupulous competitors, and criminal gangs which extort money as part of their operational model.

2. Executing security insufficiently

The first threat is paradoxically the most obvious but the least spoken of due to the fact that nobody wants to admit it. Information security does not "just happen," it is a product of serious, concerted engineering efforts with forethought and long-term planning on the part of the companies themselves. Often, however, the bare minimum of in-house effort is made to secure the IT infrastructure. Computers may be patched once during their life cycle (at time of construction) and are never again updated. (Ubuntu Server FAQ, 2012-09-09) Sometimes this is due to insufficient IT or security staffing, sometimes this is due to corporate policy (perceived risk of service disruption due to routine maintenance is dangerously high in comparison to perceived risk of a security breach), and sometimes this is due to corporate culture. In many industries there is the perception that the organization is not a target and thus security is not a priority when in fact attackers have more uses for the target's computers than the targets do. (Krebs, 2012-10-12) Some of those nefarious uses include participating in distributed denial of service botnets, hosting malware or clusters of web browser exploits, and proxying attack traffic to help conceal the locations of attackers. All

Lynch, B. A. (2016). Ongoing Threats to Emerging Financial Entities. Postmodern Openings, 7(1), 21-34. Doi: http://dx.doi.org/10.18662/po/2016.0701.02

available evidence points to the fact that any and every computer on the Net is a target for someone for any number of reasons (or no reasons at all, when automated scans of entire IP blocks are taken into account).

1.1. Symptoms

The security postures of user endpoints (workstations) rarely approximate anything that we would consider secure. In all but the most stringently controlled environments users often have administrative control over their workstations, which means that anything the user runs can impact the entire machine, including malware. Users frequently deactivate essential security measures to reduce perceived hassle or inefficiency, including local firewalls, regular automatic patching and antivirus software. OS-specific central management and orchestration systems frequently have insufficient coverage of internal networks (i.e., they silently fail to successfully push security policies or install security patches) and even repeated runs ("pushes") are rarely sufficient. (Marelia, 2011-06-14) (Microsoft, 2015-04) Blacklisting, the practice of identifying and blocking the execution of specific executables is sometimes employed as a countermeasure but is rarely effective for very long due to the rapid rate of drift of malware executables and relative ease of editing existing binaries so that they no longer match the blacklist. The security practice of whitelisting, in which all applications are prevented from executing save for a handful which are explicitly permitted by the system administrator, is used only in the highest of security environments. (Techtarget, 2011-06) Unfortunately, the trade-off of application whitelisting is that the system becomes largely useless for anything else, leading to increased IT support overhead and sometimes the whitelisting policy being rescinded.

While all of these things seem (and indeed are) simplistic, they are also the most commonly encountered root causes of severe security compromises. (ASQ, 2016) Bluntly, they are so simple that they are disregarded as being essential at all. And therein lies the most serious problem of all: Continuing to treat information security processes as nonessential. Security protocols may be ignored; security enforcing equipment may never be installed or configured; continual monitoring of systems may never occur. Any one of these things constitutes a critical error in basic security and could lead to catastrophic compromise.

Lynch, B. A. (2016). Ongoing Threats to Emerging Financial Entities. Postmodern Openings, 7(1), 21-34. Doi: http://dx.doi.org/10.18662/po/2016.0701.02

2.2. Remediation

Regardless of the availability of resources basic hardening of servers and workstations is hit or miss at best. (DISA, 2016) (NSA, 2009) (CisoFy, 2016) (OSU, 2014) At the very least the relatively significant amount of up-front effort required to harden a single system is enough to deter inexperienced system administrators; applying that amount of effort to every system in the long run is both not sustainable and risky. Applying hardening measures to any machine disables some of its functionality out of necessity due to the fact that flexibility and security have an antagonistic and inverse relationship. To this day there is the perception that instituting increased security measures on a server is more likely than not to break essential applications. This is not and never has been the case; just as operating environment hardening should be applied and documented in atomic stages, the application should be installed, configured and tested per the manufacturer's documentation, and if necessary the security hardening steps should be backed out or adjusted one at a time, documenting each modification, until the application functions normally. (Wikipedia, 2016) Once complete the documentation should be finalized so that it can be used to implement hardening protocols in an automated fashion to minimize craft error and accelerate deployment in the future.

Solving this class of problems does require a significant amount of initial effort, but in the long term the amount of work required to maintain the solutions is measurably less, especially when compared to the amount of time, energy, and money that would be applied to recovering from a security breach, including loss of business and possible legal repercussions. The long term solution starts with constructing a central system orchestration mechanism that will be used to manage every system of the enterprise, from workstations to production, staging, and development servers. (Chef, 2016) (Puppet, 2016) The server the central orchestration mechanism runs on should itself be tightly controlled and all users should multiply authenticate to it to help prevent it from being used to subvert every system under its control. For each type of operating environment (Linux, BSD, Windows, and so forth) a body of public configuration code for the orchestration mechanism has been developed and published by its user community; this body of work should be searched for appropriate implementations of hardening procedures that can be applied. (Chef Supermarket, 2016)

Lynch, B. A. (2016). Ongoing Threats to Emerging Financial Entities. Postmodern Openings, 7(1), 21-34. Doi: http://dx.doi.org/10.18662/po/2016.0701.02

(Puppet Forge, 2016) The goal is not to reinvent the wheel by writing brand new hardening scripts but to find existing implementations of best practices. As a best practice each security protocol should be audited to ensure that it carries out the appropriate tasks as expected. Every system constructed should use the orchestration mechanism to implement a process in which the bare minimum operating environment is installed and no more to minimize what can be attacked. Additionally, every system should be hardened at the same time it is constructed. System updates should be applied no less than once every day using the orchestration system to maintain the security posture of every system, and the implementation of the security protocol should be immediately re-applied to verify and ensure the security configuration. Under ideal conditions every system should be rebooted after being patched to ensure that updated libraries are loaded by applications and OS kernel patches (if any) take full effect.

Once the production and staging infrastructures are managed by the orchestration mechanism and are stable, users' workstations should then be brought under the control of the central orchestration system. (Chef Supermarket, 2016) (Sweeny, 2013) (Timberman, various dates) (Puppet Forge, 2016) Workstation-appropriate security protocols should be applied evenly, including timely installation of system updates. There remains a persistent perception that installing patches is inherently dangerous - Windows 95, unfortunately, was largely to blame for this. However, in the intervening decades the development of system updates has been highly refined. Patches that destroy workstations are rare today but 0-day vulnerabilities are not. The central orchestration system should also be used to install and manage antivirus and anti-malware software on each workstation to prevent users from tampering with it. While antivirus and anti-malware software are not perfect solutions (detection and evasion techniques employed by modern malware are highly advanced) there is no reason not to employ them as an additional layer of security to stop the attempts of relatively unsophisticated attackers. ("Safensoft", 2015) (Breeden, 2015) (Krebs, 2014)

3. Unscrupulous competitors

The second major security threat in emerging industries comes from the actions of unscrupulous business competitors. The practice of industrial espionage, thought by many to be myth or urban legend results

Lynch, B. A. (2016). Ongoing Threats to Emerging Financial Entities. Postmodern Openings, 7(1), 21-34. Doi: http://dx.doi.org/10.18662/po/2016.0701.02

in the loss of tens to hundreds of millions of dollars of revenue every year. (Penenberg, 2001) (ONCE, 2011) (FBI, 2015) (Hubbs, 2015) Industrial espionage need not take the form of midnight burglaries of offices to steal prototypes or duplicate documents though there is nothing that rules this out. It can also take the form of the collection of OSINT - open source intelligence information - information that is freely available to anyone who reads a magazine, trade journal, blog, or an interview with a corporate officer. (CIA, 2013) (Hock, 2015) Every piece of information published by a company is potentially a data point which can be used to infer business deals, unannounced projects, parts of the inner workings of services, or some of the internal structure of the company itself. OSINT can also be used to plan and direct other forms of external attack, such as social engineering attempts against personnel. To put it another way, each leaked data point is a competitor's advantage if assembled and leveraged properly.

3.1. Network infiltration and active attacks

In addition it is conceivable that a competitor may use active information security attacks against a company in an attempt to infiltrate the corporate network and locate actionable information. Attribution of attacks is difficult in the extreme, which gives unethical actors a solid advantage if they decide to commit the time and resources and accept the risk. (Kostadinov, 2013) (Schneier, 2015) The general state of information security aside, malware which captures account credentials, records network traffic, actuates cameras and microphones, and which allows remote control of infected systems may be tactically deployed to collect actionable information. Remote access malware also permits the exfiltration of files in a covert manner, either directly (downloading to the control application) or indirectly (uploading files to a remote system the attackers have access to). Social engineering, watering hole, and spear phishing attacks can be used to infiltrate surveillance or remote access malware into the workstations of personnel with privileged access. (Peters, 2015) (Invincia, 2015) (Kaspersky Lab, 2015) It is trivially easy for an attacker to spoof email from a business partner or vendor with an attached document containing malware or a link to a web page containing a cluster of web browser exploits which acts as an infection vector. The malware itself is relatively easy to acquire; malware construction kits can be found with a couple of web searches, existing professional surveillance software has been leaked and mirrored widely,

Lynch, B. A. (2016). Ongoing Threats to Emerging Financial Entities. Postmodern Openings, 7(1), 21-34. Doi: http://dx.doi.org/10.18662/po/2016.0701.02

and there are companies whose sole business model is to sell and support surveillance malware regardless of the customer's intended uses for it. (Proffitt, 2013) (Hacking Team, 2015) (FinFisher, 2015)

3.2. Countermeasures

The countermeasures for industrial espionage attempts start with carrying out due diligence, vis a vis applying the aforementioned basic security protocols to production, development and staging servers as well as workstations to prevent their compromise or at least make signs of compromise significantly easier to detect in shorter periods of time. Ensure that storage media (hard drives, flash drives, and so forth) are securely erased or physically destroyed because hosting providers occasionally re-use storage media without sanitizing it and occasionally information may still be extracted from discarded drives using forensic techniques. Also ensure that documents are shredded before disposal because dumpster diving to recover discarded information from the trash or recycling is still a useful tactic. Use caution before publishing information pertaining to the company's activities because it may leak actionable details to a competitor; those details may also provide clues to an attacker that would help them more precisely target attacks. (Dougherty, 1997) Even though it is de rigueur today to use social networking sites for software engineers to host production code, consider setting up a version control server in-house to better protect source code by storing it on machines that you fully control. (Github, 2016) (Gitolite, 2016) (Gitosis, 2016) Set up strong authentication to all servers to make it more difficult for an attacker to gain access, such as by configuring the servers to require strong passphrases and two-factor authentication. (Reinhold, 2016) (Whirlenig, 2012) (Gemalto, 2015) Train all personnel to be extremely wary of opening documents or hyperlinks sent through e-mail. Contact the purported sender through separate channels to verify the authenticity of the document or link.

Lynch, B. A. (2016). Ongoing Threats to Emerging Financial Entities. Postmodern Openings, 7(1), 21-34. Doi: http://dx.doi.org/10.18662/po/2016.0701.02

4. Criminal gangs

The third ongoing threat, which has become highly visible in recent months are attacks by net.gangs that run extortion rackets. The premise is simple: A target's public infrastructure (production network, website, or even office infrastructure) is attacked with one or more simultaneous distributed denial of service attacks. (Cid, 2015) (McKeay, 2015) The target is then contacted by the attackers and told that they must transmit a certain amount of cryptocurrency to a certain address within a certain period of time or the severity of the attacks will increase in step with the amount of the ransom with the ultimate goal of putting the target out of business. Some companies pay the ransom rapidly so that they can resume normal business while others hold out as long as they can. Some targets have gone out of business as a result of the attacks. (Cluley, 2014) So far the ransoms appear to be proportionate to what the attackers think the targets are able to pay - a target that folds before they can pay constitutes a null revenue stream as well as leaking evidence of a given team's offensive capabilities. Unfortunately, now that the profitability of the practice has been proven there is no chance that DDoS extortion will stop and the is every indication that it will continue to be a profitable black market business.

4.1. Modus operandi

The modus operandi of the extortion gangs is unique in that they appear to carry out research upon their targets' infrastructures to determine points of weakness that, when attacked with a DDoS or some form of infiltrated extortion-malware cause the most disruption in the shortest amount of time. (Holmes, 2012) Some of these targets include file servers, routers, load balancers with known upper limits, unpatched or obsolete networking equipment, and misconfigured web servers. A brief attack is employed just before contact is made to demonstrate offensive capability and start the countdown to full-scale attack. To date distributed denial of service attacks with upper limits between 500 and 700 gigabits per second have been spotted in the field, with unsubstantiated reports that a few DDoS attacks briefly spiked to one terabit per second. (Pauli, 2016) (Turton, 2014) However most attacks against relatively small entities rarely break 60 gigabits per second of attack traffic. (Greenberg, 2015) There is evidence that suggests that some of the more high profile DDoS extortion groups do not maintain their own botnets; if their usual method of operation goes awry they

Lynch, B. A. (2016). Ongoing Threats to Emerging Financial Entities. Postmodern Openings, 7(1), 21-34. Doi: http://dx.doi.org/10.18662/po/2016.0701.02

seem to respond in such a way that they attempt to get any ransom at all out of the target, possibly to pay off other groups that they are renting DDoS capacity from. (Amir, 2016) (Prince, 2015)

4.2 Response strategy

It is vital that a multi-stage response strategy be developed in advance that encompasses legal, financial, technical, and media aspects of the company for the simple fact that nothing less will work. Mitigation of denial of service extortion attempts starts with planning: Acquire the services of net.savvy legal counsel in your locale of incorporation and figure out what you can and should do. Legal counsel should assist in negotiating agreements with hosting providers ahead of time because providers may be either unable or unwilling to assist during an attack. Counsel should also help negotiate as-needed contracts with existing DDoS mitigation providers whose services can be activated during an attack. Second, in the event that you are attacked decide how much degradation of service you're willing to accept before committing to active response. Some production services will not begin to show signs of damage when hit by ten or fifteen gigabits of traffic while others will slow dangerously with a few hundred malformed or badly timed requests per second. (Cid, 2015) Ensure that the central orchestration system is both well protected and hidden from attackers because it will be vital in deploying countermeasures and reconfiguring existing services to help mitigate the attacks. Countermeasures can take the form of (but are not limited to) deploying additional network firewalls to absorb some of the traffic, configuring host-based firewalls to filter out more of the attack traffic, deploying application-layer proxies in the production network and configuring the production applications themselves for aggressive rate limiting. It may become necessary to instantiate additional production infrastructure to help absorb attack traffic; this is another task best suited to the orchestration mechanism by re-using the procedures already developed.

Disclaimer

Some of the information in this article consists of sanitized security intelligence collected and analyzed by the author's employer during the course of carrying out normal duties. No sensitive or proprietary information is disclosed. This information should not be taken as an official publication of or advice from Ripple. The author speaks for himself only in the capacity of an information security professional.

Lynch, B. A. (2016). Ongoing Threats to Emerging Financial Entities. Postmodern Openings, 7(1), 21-34. Doi: http://dx.doi.org/10.18662/po/2016.0701.02

References

American Society for Quality. What is Root Cause Analysis? Retrieved 2016-02-16 from http://asq.org/learn-about-quality/root-cause-analysis/overview/overview.html

Amir, Waqas (2016-01-06). BTCC Bitcoin Trader Confronts DDoS Attackers Like A Pro. Retrieved from https://www.hackread.com/ddos-attackers-confronted-by-btcc-bitcoin-trader/

Atomicity (database systems). In Wikipedia. Retrieved 2016-02-16 from https://en.wikipedia.org/wiki/Atomicity_%28database_systems%29

Breeden II, J. (2015-05-11). Traditional Anti-virus is Dead. Long Live the New and Improved AV. Retrieved from http://www.networkworld.com/article/2919111/security/traditional-anti-virus-is-dead-long-live-the-new-and-improved-av.html

Chef (computer software). (2016). Retrieved from https://www.chef.io/

Chef Supermarket. (2016). Retrieved from https://supermarket.chef.io/cookbooks

Chef Supermarket. (2016). Retrieved from https://www.chef.io/solutions/windows/

Cid, D. (2015-09-03). Analyzing Popular Layer 7 Application DDoS Attacks. Retrieved from https://blog.sucuri.net/2015/09/analyzing-popular-layer-7-application-ddos-attacks.html

Cid, D. (2015-12-04). Increased Popularity in DDoS Extortion Campaigns. Retrieved from https://blog.sucuri.net/2015/12/ddos-extortions-campaigns.html

Cluley, G. (2014-06-21). Internet Firm Goes Out of Business After DDoS Extortion Attack. Retrieved from http://www.welivesecurity.com/2014/06/21/internet-firm-ddos-extortion-attack/

Dougherty, R. C. (1997). Claude Shannon. Retrieved from https://www.nyu.edu/pages/linguistics/courses/v610003/shan.html

FinFisher GmbH. (2015). Retrieved from the FinFisher website https://www.finfisher.com/

Gemalto. (2015). Multi-Factor Authentication Introduction. Retrieved from http://www.safenet-inc.com/multi-factor-authentication/

Lynch, B. A. (2016). Ongoing Threats to Emerging Financial Entities. Postmodern Openings, 7(1), 21-34. Doi: http://dx.doi.org/10.18662/po/2016.0701.02

Github. (2016). Retrieved from the Github website https://github.com/
Gitolite (computer software). (2016). Retrieved from http://gitolite.com/
Gitosis (computer software). (2016). Retrieved from https://github.com/tv42/gitosis
Greenberg, Adam. (2015-09-19). Akamai Warns of Increased Activity from DDoS Extortion Group. Retrieved from http://www.scmagazine.com/akamai-warns-of-increased-activity-from-ddos-extortion-group/article/437915/
Hacking Team's commercial surveillance malware and offensive software. (computer software). (2015). Retrieved from https://github.com/hackedteam?tab=repositories
Hock, Ph.D, Randolph. (2015-08-21). Internet Tools and Resources for Open Source Intelligence. Retrieved from http://www.onstrat.com/osint/
Holmes, D. (2012-03-26). The DDoS Threat Spectrum. Retrieved from https://f5.com/zh/resources/white-papers/the-ddos-threat-spectrum
Hubbs, D. (2015-02-19). 10 of the Most Infamous Cases of Industrial Espionage. Retrieved from http://www.therichest.com/rich-list/10-of-the-most-infamous-cases-of-industrial-espionage/?view=all
Invincia. (2015). Watering Hole Attacks. Retrieved from https://www.invincea.com/use-cases/attack-techniques/watering-hole-attacks/
Kaspersky Lab. (2015). Spear Phishing Definition and Prevention. Retrieved from https://usa.kaspersky.com/internet-security-center/definitions/spear-phishing
Kostadinov, D. (2013-02-01). The Attribution Problem in Cyber Attacks. Retrieved from http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/
Krebs, B. (2012-10-12). The Scrap Value of a Hacked PC, Revisited. Retrieved from http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/
Krebs, B. (2014-05-14). Antivirus is Dead: Long Live Antivirus! Retrieved from http://krebsonsecurity.com/2014/05/antivirus-is-dead-long-live-antivirus/

Lynch, B. A. (2016). Ongoing Threats to Emerging Financial Entities. Postmodern Openings, 7(1), 21-34. Doi: http://dx.doi.org/10.18662/po/2016.0701.02

Lynis (computer software). (2016). Retrieved from https://cisofy.com/lynis/

Mar-elia, D. (2011-06-14). What's Wrong With Group Policy? Retrieved from http://windowsitpro.com/active-directory/whats-wrong-group-policy

McKeay, M. (2015-07-15). DDoS Extortion: Easy and Lucrative. Retrieved from https://securityintelligence.com/ddos-extortion-easy-and-lucrative/

Microsoft. (2015-04). WSUS Silently Fails to Synchronize Updates Released in April 2015. Retrieved from https://support.microsoft.com/en-us/kb/3058255

Network Frontiers, LLC. Retrieved 2016-02-27. Unclassified DISA FSO STIG List. Retrieved from https://www.stigviewer.com/stigs

Office of the National Counterintelligence Executive. (2011-10). Foreign Spies Stealing US Economic Secrets In Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011. Retrieved from http://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

Oklahoma State University. (2014-05-26) Hardening Guides. Retrieved from https://security.okstate.edu/content/hardening-guides

Pauli, D. (2016-01-27). 500 Gbps DDoS Attack Flattens World Record. Retrieved from http://www.theregister.co.uk/2016/01/27/500gbps_ddos_attack_flattens_world_record/

Penenberg, A. L. (2001). Spooked: Espionage in Corporate America. Perseus Books Group.

Peters, S. (2015-03-17). The 7 Best Social Engineering Attacks Ever. Retrieved from http://www.darkreading.com/the-7-best-social-engineering-attacks-ever/d/d-id/1319411

Prince, B. (2015-02-20). DDoS-For-Hire Services Cheap but Effective. Retrieved from http://www.securityweek.com/ddos-hire-services-cheap-effective

Proffitt, B. (2013-07-31). How to Build A Botnet in 15 Minutes. Retrieved from http://readwrite.com/2013/07/31/how-to-build-a-botnet-in-15-minutes

Puppet (computer software). (2016). Retrieved from https://puppetlabs.com/

Puppet Forge. (2016). Retrieved from https://forge.puppetlabs.com/

Lynch, B. A. (2016). Ongoing Threats to Emerging Financial Entities. Postmodern Openings, 7(1), 21-34. Doi: http://dx.doi.org/10.18662/po/2016.0701.02

Puppet modules for managing Mac OSX. (software). Various dates of publication. Retrieved from https://forge.puppetlabs.com/tags/osx

Reinhold, A.G. (2016-01-10). The Diceware Passphrase Homepage. Retrieved from http://world.std.com/~reinhold/diceware.html

"Safensoft". (2015-02). So, how dead is antivirus, exactly? Retrieved 2016-02-20 from https://isc.sans.edu/forums/So+how+dead+is+antivirus+exactly/529/

Schneier, B. (2015-03-09). Attack Attribution and Cyber Conflict. Retrieved from https://www.schneier.com/blog/archives/2015/03/attack_attribut_1.html

Sweeny, J. (2013-09-23). Managing Windows with Puppet. Retrieved from https://puppetlabs.com/presentations/managing-windows-puppet

Techtarget.com. (2011-06). What is application whitelisting? Retrieved fromhttp://searchsecurity.techtarget.com/definition/application-whitelisting

Timberman, J., Chef cookbooks for managing Mac OSX. (computer software). Various dates of publication. Retrieved from https://github.com/chef-osx

Turton, W. (2014-12-26). An Interview with Lizard Squad, the Hackers Who Took Down XBox Live. Retrieved fromhttp://www.dailydot.com/technology/lizard-squad-hackers/

Ubuntu Server FAQ. (2012-09-09). Retrieved from https://help.ubuntu.com/community/ServerFaq#How_does_the_package_system_.28apt.29_know_what_to_install_or_update_.28server_or_desktop_packages.29.3F

US Central Intelligence Agency. (2013-04-30). INTelligence: Open Source Intelligence. Retrieved from https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html

Lynch, B. A. (2016). Ongoing Threats to Emerging Financial Entities. Postmodern Openings, 7(1), 21-34. Doi: http://dx.doi.org/10.18662/po/2016.0701.02

US Federal Bureau of Investigation. (2015-07-23). Economic Espionage. Retrieved from https://www.fbi.gov/news/stories/2015/july/economic-espionage

US National Security Agency. (2009-01-15). Operating System Security Configuration Guides. Retrieved from https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml

Whirlenig (computer software). (2012-09-23). Retrieved from https://github.com/gardners/whirlenig

Biodata

Bryce A. Lynch heads up the Information Security team at Ripple (https://ripple.com/), a global financial settlement company in California's Bay Area which aims to make transferring money as easy as sending e-mail, giving rise to an Internet of Value (IoV). Bryce is responsible for writing policy, interfacing with business and integration partners, maintaining infrastructure, and carrying out security audits and penetration tests on a company-wide basis. Outside of work Bryce carries out information security research in a number of fields, contributes to a number of open source projects, and is the developer of Exocortex, a system of semi-autonomous software agents which collect, process, mine, and report on information collected around the world and across the Internet. Bryce uses Exocortex as a cognitive prosthesis to offload tedious, tiring, and largely boring tasks to free up his brain so he can work on more interesting and challenging problems in the world. Bryce is a many-time speaker, having presented at George Mason University, the University of Maryland, Hackers On Planet Earth, F/OSScon, CarolinaCon, IS4CWN, and ICCM among other colleges and conferences around the globe.

Acknowledgment: *This the paper was presented within the ICT Fest Nigeria.*

Lynch, B. A. (2016). Ongoing Threats to Emerging Financial Entities. Postmodern Openings, 7(1), 21-34. Doi: http://dx.doi.org/10.18662/po/2016.0701.02