Infection Vectors - Risk Factors for Financial Transactions

Mircea Constantin ŞCHEAU[1], Liviu ARSENE[2], Gerald DINCĂ[3]

[1]BCR, Romania, [2]Bitdefender, Romania, [3]ARB, Romania
mirceascheau@hotmail.com, arsene.liviu@gmail.com, gerald.dinca@gmail.com

Abstract

With the proliferation of internet-enabled services and data availability, cyberattacks have become in the past decade. Relying on various techniques to either penetrate critical network infrastructures or deliver malicious payloads to unsuspecting victims, the main motivation behind most attacks is not just money but information. From banks to vendors and end users, the communication and transmission medium used for implementing safe transactions has become both complex and more prone to intrusions.

Index terms: malware, infection vector, vulnerabilities, financial institution, browser

References:

[1]. Bitdefender, (2015, 09 July), Un nou val de mesaje ce conțin un virus bancar vizează clienții băncilor din România, [Online]. Available: http://www.bitdefender.ro/news/un-nou-val-de-mesaje-ce-contin-un-virus-bancar-vizeaza-clientii-bancilor-din-romania-3058.html

[2]. Federal Bureau of Investigation, Financial Services Information Sharing and Analysis Center (FS-ISAC), Internet Crime Complaint Center (IC3), Fraud Alert – Cyber Criminals Targeting Financial Institution Employee Credentials to Conduct Wire Transfer Fraud, 2012, [Online]. Available: http://www.ic3.gov/media/2012/FraudAlertFinancialInstitutionEmployeeCredentialsTargeted.pdf

[3]. FISMA, Annual Report to Congress: Federal Information Security Management Act, 2013, [Online]. Available: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy_2013_fisma_report_05.01.2014.pdf

[4]. Kaspersky, (2015, February 18), Carbanak APT The Great Robbery, [Online]. Available: http://krebsonsecurity.com/wp-content/uploads/2015/02/Carbanak_APT_eng.pdf

[5]. Kaspersky, (2015, February 21), Carbanak APT The Great Bank Robbery, [Online]. Available: http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Carbanak_APT_eng.pdf

[6]. Limburger, Bedrijfsspionage bij DSM via usb-sticks, 2012, [Online]. Available: http://www.limburger.nl/article/20120707/REGIONIEUWS01/120709723

[7]. NIST, Framework for Improving Critical Infrastructure Cybersecurity, 2014, [Online]. Available: http://www.nist.gov/cyberframework/

[8]. PCI Security Standards Council, Payment Card Industry (PCI) Data Security Standard, 2015, [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

[9]. Ponemon Institute, The Challenge of Preventing Browser-Borne Malware, 2015, [Online]. Available: http://learn.spikes.com/rs/spikessecurity/images/Ponemon-Spikes-Report.pdf

[10]. Radicati Group Inc, E-mail Statistics Report, 2015, [Online]. Available: http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf

[11]. SANS, Security Spending and Preparedness in the Financial Sector: A SANS Survey, 2015, [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/security-spending-preparedness-financial-sector-survey-36032

[12]. SANS, Critical Security Controls for Effective Cyber Defense, [Online]. Available: https://www.sans.org/critical-security-controls/

[13]. The Intercept, Secret Malware in European Union Attack Linked to U.S. and British Intelligence, 2014, [Online]. Available: https://firstlook.org/theintercept /2014/11/24/secret-regin-malware-belgacom-nsa-gchq/

[14]. Trend Micro Incorporated, Russian Underground 101, 2012, [Online]. Available: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

[15]. Verizon, 2015 Data Breach Investigations Report, 2015, [Online]. Available: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf

[16]. Wired, (2015, February 16), Suite of Sophisticated Nation-State Attack Tools Found With Connection to Stuxnet, [Online]. Available: http://www.wired.com/2015/02/kapersky-discovers-equation-group/

[17]. Romanian National Computer Security Incident Response Team, Security Reports, [Online]. Available: http://www.cert.ro