**REFERENCES**

[1] Gnu octave: high-level interpreted language. http://www.gnu.org/

software/octave/.

[2] hphosts, a community managed hosts file. http://hphosts.gt500.org/hosts.

txt.

[3] Joewein.de LLC blacklist. http://www.joewein.net/dl/bl/dom-bl-base.

txt.

[4] Lookout. https://play.google.com/store/apps/details?hl=en&id=com.

lookout.

[5] Malware Domains List. http://mirror1.malwaredomains.com/files/

domains.txt.

[6] Phishtank. http://www.phishtank.com/.

[7] Pindrop phone reputation service. http://pindropsecurity.com/

phone-fraud-solutions/phone reputation service prs/.

[8] Scrapy — an open source web scraping framework for python. http://

scrapy.org/.

[9] VirusTotal. https://www.virustotal.com/en/.

[10] Google developers: Safe Browsing API. https://developers.google.com/

safe-browsing/, 2012.

[11] Alexa, the web information company. http://www.alexa.com/topsites,

2013.

[12] dotmobi. internet made mobile. anywhere, any device. http://dotmobi.

com/, 2013.

[13] C. Amrutkar, K. Singh, A. Verma, and P. Traynor. VulnerableMe: Measuring

systemic weaknesses in mobile browser security. In Proceedings of the

International Conference on Information Systems Security (ICISS), 2012.

[14] C. Amrutkar, P. Traynor, and P. C. van Oorschot. Measuring SSL indicators

on mobile browsers: Extended life, or end of the road? In Proceedings of the

Information Security Conference (ISC), 2012.

[15] M. Antonakakis, R. Perdisci, D. Dagon, W. Lee, and N. Feamster. Building

a dynamic reputation system for DNS. In Proceedings of the 19th USENIX

Conference on Security (SECURITY), 2010.

[16] V. A. Balasubramaniyan, A. Poonawalla, M. Ahamad, M. T. Hunter, and

P. Traynor. Pindr0p: using single-ended audio features to determine call

provenance. In Proceedings of the 17th ACM Conference on Computer and

Communications Security (CCS), 2010.

[17] L. Bilge, E. Kirda, C. Kruegel, and M. Balduzzi. EXPOSURE : Finding

malicious domains using passive DNS analysis. In Proceedings of the 18th

Annual Network and Distributed System Security Symposium (NDSS), 2011.

[18] M. Boodaei. Mobile users three times more vulnerable to phishing attacks.

http://www.trusteer.com/blog/mobile-users-threetimes-

more-vulnerable-to-phishing-attacks, 2011.

[19] M. Butkiewicz, Z. Wu, S. Li, P. Murali, V. Hristidis, H. V. Madhyastha,

and V. Sekar. Enabling the transition to the mobile web with websieve. In

Proceedings of the 14thWorkshop on Mobile Computing Systems and Applications

(HotMobile), 2013.

[20] D. Canali, M. Cova, G. Vigna, and C. Kruegel. Prophiler: a fast filter for

the large-scale detection of malicious web pages. In Proceedings of the 20th

International Conference on World Wide Web (WWW), 2011.

[21] S. Chakradeo, B. Reaves, P. Traynor, andW. Enck. MAST: Triage for Marketscale

Mobile Malware Analysis. In Proceedings of the ACM Conference on

Security and Privacy in Wireless and Mobile Networks (WiSec), 2013.

[22] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In Proceedings

of the SIGCHI Conference on Human Factors in Computing Systems, 2006.

[23] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri. A study of Android

application security. In Proceedings of the 20th USENIX Security Symposium,

2011.

[24] B. Feinstein and D. Peck. Caffeine monkey: Automated collection, detection

and analysis of malicious javascript. In Proceedings of the Black Hat Security

Conference, 2007.

[25] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner. Android permissions

demystified. In Proceedings of the 18th ACM conference on Computer and

communications security, 2011.

[26] A. P. Felt and D. Wagner. Phishing on mobile devices. In Web 2.0 Security

and Privacy (W2SP), 2011.

[27] A. P. Felt, H. J. Wang, A. Moshchuk, S. Hanna, and E. Chin. Permission

re-delegation: attacks and defenses. In Proceedings of the 20th USENIX

conference on Security, 2011.

[28] I. Fette, N. Sadeh, and A. Tomasic. Learning to detect phishing emails. In

Proceedings of the 16th International Conference on World Wide Web (WWW),

2007.

[29] S. Gajek, A.-R. Sadeghi, C. St ¨ uble, and M. Winandy. Compartmented

security for browsers or how to thwart a phisher with trusted computing.

In Second International Conference on Availability, Reliability and Security

(ARES), 2007.

[30] S. Garera, N. Provos, M. Chew, and A. D. Rubin. A framework for detection

and measurement of phishing attacks. In Proceedings of the ACM workshop

on recurring malcode, 2007.

[31] T. Holz, C. Gorecki, K. Rieck, and F. C. Freiling. Measuring and detecting

fast-flux service networks. In Proceedings of the Network and Distributed

System Security Symposium (NDSS), 2008.

[32] A. Ikinci, T. Holz, and F. Freiling. Monkey-spider: Detecting malicious

websites with low-interaction honeyclients. In Proceedings of Sicherheit,

Schutz und Zuverlassigkeit, 2008.

[33] L. Invernizzi, S. Benvenuti, M. Cova, P. M. Comparetti, C. Kruegel, and

G. Vigna. Evilseed: A guided approach to finding malicious web pages. In

Proceedings of the 2012 IEEE Symposium on Security and Privacy, 2012.

[34] P. Kolari, T. Finin, and A. Joshi. Svms for the blogosphere: Blog identification

and splog detection. In Proceedings of AAAI Spring Symposium on

Computational Approaches to Analysing Weblogs, 2006.

[35] A. Le, A. Markopoulou, and M. Faloutsos. Phishdef: Url names say it all.

In Proceedings of IEEE International Conference on Computer Communications

(INFOCOM), 2011.

[36] C. Lever, M. Antonakakis, B. Reaves, P. Traynor, and W. Lee. The core of

the matter: Analyzing malicious traffic in cellular carriers. In Proceedings

of Network and Distributed System Security Symposium (NDSS), 2013.

[37] P. Likarish, E. Jung, and I. Jo. Obfuscated malicious javascript detection

using classification techniques. In Proceedings of Malicious and Unwanted

Software (MALWARE), 2009.

[38] C. Ludl, S. Mcallister, E. Kirda, and C. Kruegel. On the effectiveness of

techniques to detect phishing sites. In Proceedings of the 4th International

Conference on Detection of Intrusions and Malware, and Vulnerability Assessment

(DIMVA), 2007.

[39] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker. Beyond blacklists: Learning

to detect malicious web sites from suspicious URLs. In Proceedings of the

SIGKDD Conference, 2009.

[40] D. K. McGrath and M. Gupta. Behind phishing: an examination of phisher

modi operandi. In Proceedings of the 1st Usenix Workshop on Large-Scale

Exploits and Emergent Threats (LEET), 2008.

[41] E. Medvet, E. Kirda, and C. Kruegel. Visual-similarity-based phishing

detection. In Proceedings of International Conference on Security and Privacy

in Communication Netowrks (SecureComm), 2008.

[42] Y. min Wang, D. Beck, X. Jiang, R. Roussev, C. Verbowski, S. Chen, and

S. King. Automated web patrol with strider honeymonkeys: Finding web

sites that exploit browser vulnerabilities. In Proceedings of the Networking

and Distributed Systems Security (NDSS), 2006.

[43] A. Mohaisen and O. Alrawi. AV-Meter: An Evaluation of Antivirus Scans

and Labels. In Proceedings of the 4th International Conference on Detection of

Intrusions and Malware, and Vulnerability Assessment (DIMVA), 2014.

[44] T. Moore, R. Clayton, and H. Stern. Temporal correlations between spam

and phishing websites. In Proceedings of the 2nd USENIX conference on Largescale

exploits and emergent threats: botnets, spyware, worms, and more (LEET),

2009.

[45] A. Moshchuk, T. Bragin, S. D. Gribble, and H. M. Levy. A crawler-based

study of spyware on the web. In Proceedings of Network and Distributed

System Security Symposium (NDSS), 2006.

[46] J. Nazario. Phoneyc: a virtual client honeypot. In Proceedings of the

2nd USENIX conference on Large-scale Exploits and Emergent Threats: botnets,

spyware, worms, and more (LEET), 2009.

[47] J. Nazario and T. Holz. As the net churns: Fast-flux botnet observations. In

Proceedings of 3rd International Conference on Malicious and Unwanted Software

(MALWARE), 2008.

[48] E. Passerini, R. Paleari, L. Martignoni, and D. Bruschi. Fluxor: Detecting

and monitoring fast-flux service networks. In Proceedings of the 5th International

Conference on Detection of Intrusions and Malware, and Vulnerability

Assessment (DIMVA), 2008.

[49] R. Perdisci, I. Corona, D. Dagon, and W. Lee. Detecting malicious flux

service networks through passive analysis of recursive DNS traces. In

Proceedings of Annual Computer Security Applications Conference (ACSAC),

2009.

[50] G. Podjarny. Mobile web performance optimization.

http://www.slideshare.net/blazeio/

mobile-web-performance-optimization-tips-and-tricks.

[51] N. Provos, P. Mavrommatis, M. A. Rajab, and F. Monrose. All your

iframes point to us. In Proceedings of the 17th USENIX conference on Security

(SECURITY), 2008.

[52] L. Rodgers and W. A. Nicewander. Thirteen ways to look at the correlation

coefficient. The American Statistician, 1988.

[53] C. Seifert, I. Welch, and P. Komisarczuk. Identification of malicious web

pages with static heuristics. In Telecommunication Networks and Applications

Conference, 2008.

[54] F. Weimer. Passive DNS replication. 2005.

[55] C. Whittaker, B. Ryner, and M. Nazif. Large-scale automatic classification

of phishing pages. In Proceedings of the Networking and Distributed Systems

Security (NDSS), 2010.

[56] G. Xiang, J. Hong, C. P. Rose, and L. Cranor. Cantina+: A feature-rich

machine learning framework for detecting phishing web sites. ACM

Transactions on Information and System Security (TISSEC), 14(2), Sept. 2011.

[57] C. Yue and H. Wang. Characterizing insecure javascript practices on the

web. In Proceedings of the 18th international conference on World Wide Web

(WWW), 2009.

[58] B. Zdrnja, N. Brownlee, and D. Wessels. Passive monitoring of DNS

anomalies. In Proceedings of the 4th International Conference on Detection of

Intrusions and Malware, and Vulnerability Assessment (DIMVA), 2007.

[59] Y. Zhang, J. I. Hong, and L. F. Cranor. Cantina: a content-based approach

to detecting phishing web sites. In Proceedings of the 16th international

conference on World Wide Web (WWW), 2007.