Looking Into a Cyber-Attack Facilitator in the Netherlands

Appendix

TrendLabs Security Intelligence Blog

April 2016

Related URLs:

Date	IP address	Domain	Actor	Description
Apr-2016	185.117.[xx].20	catholicsinaliance.org	Pawn Storm	Exploit used in targeted attacks
	131.72.[xxx].204	localiser-icloud.com	unknown	Apple ID phishing
	131.72.[xxx].174	inside-apple-localisation.com	unknown	Apple ID phishing
	131.72.[xxx].174	inside-localisation-apple.com	unknown	Apple ID phishing
Mar-2016	185.141.[xx].191	account-web.de	unknown	German freemail phishing
	185.82.[xxx].108	securityicloudservice.com	unknown	Apple ID phishing
	185.45.[xxx].218	bestapplestore.com	unknown	Apple ID phishing
	185.117.[xx].154	wsjworld.com	Pawn Storm	Exploit used in targeted attacks
	185.117.[xx].154	worldpoliticsreviews.com	Pawn Storm	Exploit used in targeted attacks
	185.117.[xx].5	mailhost.university-tartu.info	Pawn Storm	Credential phishing against Estonian university
	185.82.[xxx].146	mail.armf.bg.message-id8665213.tk	Pawn Storm	Credential phishing against Bulgarian army
	131.72.[xxx].123	loqin-yandex.ru	Pawn Storm	Credential phishing against Russian domestic targets
	131.72.[xxx].137	setting-mail.ru	Pawn Storm	Credential phishing against Russian domestic targets
Feb-2016	185.130.[x].72	play.gooqle.eu.com	unknown	Banking malware targeting Russia
	131.72.[xxx].200	eposta.basbakanlik.qov.web.tr	Pawn Storm	Credential phishing against Turkish government
	131.72.[xxx].154	poczta.mon-gov.pl	Pawn Storm	Credential phishing against Polish government
	185.117.[xx].147	yahoo.securepassword.info	Pawn Storm	US freemail phishing
	131.72.[xxx].114	posta-hurriyet.com	Pawn Storm	Credential phishing against Turkish media
	131.72.[xxx].200	tbmm.qov.web.tr	Pawn Storm	Credential phishing against Turkish government
	185.106.[xxx].251	mailhost-ut.ee	Pawn Storm	Credential phishing against Estonian university
	131.72.[xxx].55	privacy-facebook.me	Pawn Storm	Credential phishing against Facebook users
	131.72.[xxx].114	mail-hurriyet.com	Pawn Storm	Credential phishing against Turkish media

Date	IP address	Domain	Actor	Description
	131.72.[xxx].137	setting-mail.ru	Pawn Storm	Credential phishing against Russian domestic targets
	131.72.[xxx].104	tbmm.qov.web.tr	Pawn Storm	Credential phishing against Turkish government
	185.82.[xxx].88	cc-yahoo-inc.org	Pawn Storm	Credential phishing against US company
	131.72.[xxx].200	e-post.byegm.web.tr	Pawn Storm	Credential phishing against Turkish government
Jan-2016	185.117.[xx].116	marktingvb.ml	DustySky	C&C
	131.72.[xxx].200	mail.byegm.web.tr	Pawn Storm	Credential phishing against Turkish government
Dec-2015	131.72.[xxx].189	mail.mofa.g0v.qa	Pawn Storm	Credential phishing against Qatari government
	131.72.[xxx].179	webmail-gov.me	Pawn Storm	Credential phishing against Montenegrin government
	185.82.[xxx].102	redirect2app.cf	Pawn Storm	US freemail phishing
	131.72.[xxx].165	-	Pawn Storm	C&C
	131.72.[xxx].129	-	DustySky	Spear-phishing mails' source
Nov-2015	185.45.[xxx].227	-	unknown	Spear-phishing mails' source
	131.72.[xxx].129	-	DustySky	Spear-phishing mails' source
	131.72.[xxx].67	int-live.com	Pawn Storm	US freemail phishing
	131.72.[xxx].137	options-mail.ru	Pawn Storm	Credential phishing against Russian domestic targets
	131.72.[xxx].150	mycloud-mail.ru	Pawn Storm	Credential phishing against Russian domestic targets
	131.72.[xxx].162	mail.g0v.me	Pawn Storm	Credential phishing against Montenegrin government
	185.45.[xxx].238	mail-navy.ro	Pawn Storm	Credential phishing against Romanian government
	185.82.[xxx].217	iraqinews.info	Pawn Storm	Exploit used in targeted attacks
	131.72.[xxx].184	mail-justus.com.ua	Pawn Storm	Credential phishing against Ukrainian company
	185.82.[xxx].217	reuters-press.com	Pawn Storm	Exploit used in targeted attacks
	185.82.[xxx].102	help-yahoo-service.com	Pawn Storm	US freemail phishing

Date	IP address	Domain	Actor	Description
Oct-2015	185.82.[xxx].251	mail.kuwaitarmy.gov-kw.com	Pawn Storm	Credential phishing against Kuwaiti government
	185.82.[xxx].194	int-live.com	Pawn Storm	US freemail phishing
	185.82.[xxx].174	nato-news.com	Pawn Storm	Exploit used in targeted attacks
	131.72.[xxx].196	webmail.mofa.qov.ae	Pawn Storm	Credential phishing against the UAE government
	185.45.[xxx].63	mailmil.ae	Pawn Storm	Credential phishing against the UAE government
	131.72.[xxx].9	mail.rsaf.qov.sa.com	Pawn Storm	Credential phishing against Saudi Arabian government
Sep-2015	131.72.[xxx].33	-	Pawn Storm	C&C
	185.106.[xxx].75	mail.teiecomitalia.it	Pawn Storm	Italian freemail phishing
	185.82.[xxx].246	-	Pawn Storm	Credential phishing against MH17 investigation team
	185.82.[xxx].194	live-settings.com	Pawn Storm	US freemail phishing
	131.72.[xxx].131	military-info.eu	Pawn Storm	Exploit used in targeted attacks
Aug-2015	185.82.[xxx].174	electronicfrontierfoundation.org	Pawn Storm	Exploit used in targeted attacks
	185.82.[xxx].174	osce-press.com	Pawn Storm	Exploit used in targeted attacks
	185.82.[xxx].11	electronicfrontierfoundation.org	Pawn Storm	Exploit used in targeted attacks
	185.45.[xxx].125	grab2d.com	unknown	Credential phishing against the UAE government
	185.82.[xxx].159	bit2ly.com	Pawn Storm	Credential phishing against US company
	185.82.[xxx].194	blu172maillive.com	Pawn Storm	US freemail phishing
	185.106.[xxx].220	mobile-sanoma.net	Pawn Storm	Credential phishing against Finnish company
Jul-2015	185.45.[xxx].125	grab2d.com	unknown	US freemail phishing
	185.106.[xxx].208	euroreport24.com	Pawn Storm	Exploit used in targeted attacks
	185.82.[xxx].110	service-ukr.net	Pawn Storm	Ukrainian freemail phishing
	185.82.[xxx].102	edit-mail-yahoo.com	Pawn Storm	US freemail phishing
	131.72.[xxx].204	accounts-updated-confirmation.com	unknown	Credential phishing against the UAE government

Date	IP address	Domain	Actor	Description
	131.72.[xxx].41	pasport-yandex.ru	Pawn Storm	Credential phishing against Russian domestic targets
	131.72.[xxx].41	rn-mail.ru	Pawn Storm	Credential phishing against Russian domestic targets
	131.72.[xxx].10	eservicesystems.net	Pawn Storm	C&C
	185.45.[xxx].69	defensenews.org	Pawn Storm	Exploit used in targeted attacks
	185.45.[xxx].69	aijazeera.org	Pawn Storm	Exploit used in targeted attacks
Jun-2015	185.45.[xxx].33	service-yahoo.com	Pawn Storm	US freemail phishing
	131.72.[xxx].33	itunes-helper.net	Pawn Storm	C&C
	185.45.[xxx].175	unbulletin.com	Pawn Storm	Exploit used in targeted attacks
May-2015	185.45.[xxx].175	mfagreece.com	Pawn Storm	Exploit used in targeted attacks
	185.45.[xxx].175	osce-info.com	Pawn Storm	Exploit used in targeted attacks
	131.72.[xxx].245	-	Pawn Storm	Spear-phishing mails' source
	185.45.[xxx].33	privacy-yahooservice.com	Pawn Storm	US freemail phishing
	131.72.[xxx].185	webmail-mil.gr	Pawn Storm	Credential phishing against Greek government

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

Securing Your Journey to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003