

How Cyber Propaganda Influenced Politics in 2016

Appendix

TrendLabs Security Intelligence Blog

January 2017

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

List of the targets

The following table lists entities and organizations we have observed to have been targeted by Pawn Storm.

Date	Organization	Phishing URL
Military		
12-Dec-13	Chilean military	mail.fach.rnil.cl
15-May-14	Armenian military	mail.rnil.am
23-Oct-14	Latvian military	web.mailmil.lv
25-Feb-15	Romanian military	fortele.ro
25-Mar-15	Danish military	webmail-mil.dk
26-Mar-15	Portuguese military	webmail.exercito.pt
13-May-15	Greek military	webmail-mil.gr
04-Sep-15	Danish military	fkit-mil.dk
05-Sep-15	Saudi military	mail.rsaf.gov.sa.com
16-Oct-15	United Arab Emirates army	www.mailmil.ae
19-Oct-15	Kuwaiti military	mail.kuwaitarmy.gov-kw.com
21-Oct-15	Romanian military	mail-navy.ro
04-Mar-16	Bulgarian military	mail.armf.bg.message-id8665213.tk
Ministry of Defense		
23-Jan-14	MOD of Bulgaria	mail.arnf.bg
11-Feb-14	MOD of Poland	poczta.mon.q0v.pl
04-Apr-14	MOD of Hungary	mail.hm.qov.hu
30-Apr-14	MOD of Albania	mod.qov.al
22-May-14	MOD of Spain	mail.mod.qov.es
18-Nov-14	MOD of Afghanistan	mail.mod.qov.af
05-Sep-15	MOD of Saudi Arabia	mail.moda.qov.sa.com
19-Feb-16	MOD of Poland	poczta.mon-gov.pl
Ministry of Foreign Affairs		
17-Mar-15	MFA of South Georgia	email.mfa.qov.gs
16-Jul-15	MFA of Armenia	webmail-mfa.am
02-Oct-15	MFA of the United Arab Emirates	webmail.mofa.qov.ae
02-Oct-15	MFA of the United Arab Emirates	webmail.mfa.qov.ae
10-Dec-15	MFA of Qatar	mail.mofa.g0v.qa
Intelligence Units		
10-Jan-14	State Agency for National Security (Bulgaria)	dansa.bg
Defense Industry		
24-Apr-14	Academi	mail.academl.com
24-Apr-14	Boston Dynamics	mail.bostondynamlcs.com
11-Aug-14	SAIC	webmail-saic.com
10-Sep-14	Polski Holding Obronny	mailpho.com
Media		
01-Nov-14	New York Times	privacy-yahoo.com
01-Dec-14	New York Times	link.candybober.info

Date	Organization	Phishing URL
24-Aug-15	Sanoma Media	mobile-sanoma.net
24-Feb-16	Hurriyet	posta-hurriyet.com
14-Mar-16	Anadolu Agency	anadolu-ajansi.com
15-Mar-16	Anadolu Agency	mail.anadoluajansi.web.tr
11-May-16	Hurriyet	webmail-hurriyet.com
12-Jun-16	Hurriyet	mail-hurriyet.com
14-Nov-16	Al Jazeera	account-aljazeera.net
14-Nov-16	Al Jazeera	ssset-aljazeera.net
15-Nov-16	Al Jazeera	sset-aljazeera.net
16-Nov-16	Al Jazeera	sset-aljazeera.com
21-Nov-16	Al Jazeera	mail-aljazeera.net
Politics		
12-Jan-16	Prime Minister of Turkey	e-post.byegm.web.tr
12-Jan-16	Prime Minister of Turkey	mail.byegm.web.tr
01-Feb-16	Prime Minister of Turkey	eposta.basbakanlik.qov.web.tr
01-Feb-16	Parliament of Turkey	e-posta.tbmm.qov.web.tr
01-Mar-16	Democratic Party (US)	myaccount.google.com-securitysettingpage.gq
01-Apr-16	Democratic Party (US)	myaccount.google.com-changepasswordmyaccount-idx8jxcn4ufdmncudd.gq
22-Apr-16	CDU (Germany)	webmail-cdu.de
06-May-16	CDU (Germany)	support-cdu.de
06-Jun-16	Democrat Party (US)	actblues.com
20-Oct-16	Parliament of Montenegro	mail-skupstina.me
Academics		
04-Mar-16	Tartu University	mail.university-tartu.info
Government Agencies		
24-May-15	Government of Montenegro	mail-gov.me
14-Sep-15	Safety Board Netherlands	vpn.onderzoekraad.nl
28-Sep-15	Safety Board Netherlands	sftp.onderzoekraad.nl
03-Nov-15	Government of Montenegro	mail.g0v.me
Energy		
10-Dec-14	Westinghouse Nuclear	webmail.westinghousenuclear.com
International Organizations		
18-Jun-14	Organization for Security and Co-operation in Europe	login-osce.org
23-Apr-15	Partnership for Peace Information Management System	mail-pims.org
03-Aug-16	World Anti-Doping Agency	mail.wada-awa.org
08-Aug-16	World Anti-Doping Agency	inside.wada-arna.org
08-Aug-16	Court of Arbitration for Sport	tas-cass.org

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.

©2017 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.



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