TREND MICRO | research

Water Pamola Attacked Online Shops Via Malicious Orders

By Jaromir Horejsi and Joseph C Chen

APPENDIX

Indicators of Compromise (IoCs)

SHA-256 Hashes

SHA-256	Filename	Detection Name	Type
d7517ccd8f8ab7388867da27b8d84aaf2665449580beebcdb9b3ab9141ffee9c	アンケート調査活動.lnk	Trojan.LNK.ZEGOST.AA	LNK file
8ef70e436253632ba71da8228de7d7683cfba6838f597084dd7944116835839b	update.msi	Trojan.Win32.ZEGOST.I	MSI Loader
aa6646bcb2a649fb3187de368dc6db0df169eade6a58b7c41c4451a78574e259	update.msi	Trojan.Win32.ZEGOST.I	MSI Loader
3cedbaa1b5de06beeb63e62582089eabd9da2d9f0d100582645246d1310f5d75		Trojan.JS.EXESES.AA	XSS Attack Script
3dab67781437402a8080ac64adc43959624404c659fc5de21e0ab9e29a33a1cf		Trojan.JS.EXESES.AA	XSS Attack Script
3eaecee7c3bfdbba658bd4e342654bf2e42d75956b11127bf1ac548d124aaa73		Trojan.JS.EXESES.AA	XSS Attack Script
9ee9c481eae311269d348619a2b7f7b32fe3b835529e09f297c4616923d7a5f8		Trojan.JS.EXESES.AA	XSS Attack Script
22a1fbb471b6c8bd18c855b1ba5bade95dea3348e37f882888b8787d16cd7cc9		Trojan.JS.EXESES.AA	XSS Attack Script
219cfe027c74e4445ca0bf301dc321a2091b227aaf59adc6d85476f4c7a27309		Trojan.JS.EXESES.AA	XSS Attack Script
797b4e70e4f8a9163d0ac190dfb5f52e1be842a0cd7deee9bab656e6445cd1e		Trojan.JS.EXESES.AA	XSS Attack Script
23205e5e648777edc0b9de757b052062263285636926fd0dcb2e64105a36c939		Trojan.JS.EXESES.AA	XSS Attack Script
24444b363fb88c8b7e4889c9df69d0b12cb69824ad7820be5e3887fd6f6989f9		Trojan.JS.EXESES.AA	XSS Attack Script
751867d2963c9e842e7d6312a597ed3d39b7d4366c4e57ee9939ac6efa840776		Trojan.JS.EXESES.AA	XSS Attack Script
a58b6a628dc1baefd85309dff389e149a202213943ba40a20e4dc25f44820226		Trojan.JS.EXESES.AA	XSS Attack Script
a88da6e48cc296918acff1a7501e128a48033f3c14d50033aca40e5221cdff5e		Trojan.JS.EXESES.AA	XSS Attack Script
cd1e4892d3768b6499170d5557e740ecaa9c5c8f0397f540395b443f22266fda		Trojan.JS.EXESES.AA	XSS Attack Script
ceeefaf53449e5305f8ee3715ed59a38a06be0b52865baad334d43c2fcdf9989		Trojan.JS.EXESES.AA	XSS Attack Script
d2f63f3491b501cb03253f80725742f555e794bc69e8f5150269ae6c0a88b8ac		Trojan.JS.EXESES.AA	XSS Attack Script
d8e5c842676fcc3bfc074c75e7d129b08983a8ac6eeb5a0a5fbddee22fb19735		Trojan.JS.EXESES.AA	XSS Attack Script

d37b1085371fa4df052c9f863a2ca05ec2cb491b8c68e037e877f521806cc993		Trojan.JS.EXESES.AA	XSS Attack Script
e63292167d8e1ae655a302921a442596ad94797d694c3827c1aec2721eb88348		Trojan.JS.EXESES.AA	XSS Attack Script
191d2ca5938eb990fe50e93287d37115249d6ed7fcd0ec18cbf326c96dba0f60		Trojan.JS.EXESES.AA	XSS Attack Script
f219d13c38636a2855cd5645018b708b48d098ecd1b4d1a6a8ff7bbd5e92c669	MakePlugin.tar.gz	Backdoor.PHP.WEBSHELL.SBJKVC	Malicious Plugin of E-commerce Platform
d4f7b6db3e4c9dd0a99eadafebc213143df3ee8e4f65d42fede066de3b17b541	Adobe_Air_32.0_for_Win.zip	Trojan.Win32.MAKOOB.AW	Fake Flash Installer Archive
50eb560d3752212e0a238dc0570f2c962e358344b00e40486d9fab2333c23b64	Adob.dll	Trojan.Win32.MAKOOB.AW	Fake Flash Installer Archive
ce3741698c8dd5bdbd59e790c79c33de64c3317c01b3333d47ba941e46678c7b	ulibs.dll	Trojan.Win32.MAKOOB.AW	DLL Loader
e0681150926a131959aa5d54288ad10b3307ad9860912745f9238768ecc0451c	oplib.dll	Trojan.Win32.MAKOOB.AW	DLL Loader
f8e16a43e966e52df1ced8a475d3ae8df8e5a8822e13e77127b4f4adcafec411	oplib.dll	Trojan.Win32.MAKOOB.AW	DLL Loader
ba805ab2097bd9dda318cc7fe43fba5f36df6d9f9ea5c28334142424fb20b088	oplib.dll	Trojan.Win32.MAKOOB.AW	DLL Loader
ce264e323ef623d4b06e78da04ab0e59d5b456bd2a3590f4a084d4de3e65470e	lib.DAT	Trojan.Win32.MAKOOB.AW.enc	Encrypted Payload
d55ab5acefe307b68825d214e1f2f58f50a9ef865d1f8b83477fa1c01537f369	lib.DAT	Trojan.LNK.ZEGOST.AA.enc	Encrypted Payload
5e11b0f22ee12c649dd175b5b566c621cecc53bfa3d26dab9ec295b1e125a1f1		Backdoor.Win32.FARFLI.RGJ	Gh0st RAT
7a69262f70b6e27dc1e04ac678b2ff4f39d3049b4d3504cf91eb9e2bd17f2b60		Backdoor.Win32.FARFLI.RGJ	Gh0st RAT
c758267023452e257d5469269300ad8add92a888fadd01e21ca1f69910c32142		Backdoor.Win32.FARFLI.RGJ	Gh0st RAT
1d0f588190c3e5190c967b3aefca36f793075ec17162a553a7dda21abb525aac		Backdoor.Win32.FARFLI.RGJ	Gh0st RAT

Gh0stRat URLs

URL	Category
mail[.]update—microsoft[.]com	C&C Server
online[.]update—microsoft[.]com	C&C Server

Water Pamola Domains

URL	Category
adobe-air[.]com	Phishing
cloudlstorage[.]com	Phishing
basic-authentication[.]live	Phishing
auth1html[.]site	Phishing
googleoapis[.]com	Phishing
xf6[.]site	Phishing
77i[.]co	Phishing

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com