NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

January 20, Edition 1.0

NETWORK INTELLIGENCE SECURITY ADVISORY

The major security news items of the month - major threats and security patch advisory. The advisory also includes IOCs and remediation steps.

IN THIS EDITION:

Security Advisory Listing	Severity
FIN8 Threat Actors found targeting Point-of-Sales (POS) systems for stealing payment card data from Retailers and Fuel Dispenser Merchants, on global scale.	High
Rancor, a Chinese-based Cyber Espionage Group found using customized malware and exploits, to target organizations in South-East Asia and other regions on global scale	High
Ukraine-based Threat Actors found targeting organizations using sophisticated Carbanak Backdoor	Critical
An exploitable Remote Code Execution vulnerability (CVE-201910758) found in MongoDB Mongo-Express, which can allow a remote attacker to execute arbitrary code on the affected system	Critical

ALSO INSIDE

Security Patch Advisory

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

FIN8 Threat Actors found targeting Point-of-Sales (POS) systems for stealing payment card data from Retailers and Fuel Dispenser Merchants, on global scale.

Severity: High

Date: December 18, 2019

IP ADDRESSES

- 162.243.40.7
- 192.64.119.98
- 157.230.233.65
- 134.209.78.73
- 185.159.131.11
- 45.77.152.39

DOMAINS

- Troxymuntisex.org
- Nduropasture.net
- Diolucktrens.org
- Fraserdolx.org

REMEDIATION

1. Immediately apply Security Patches for Microsoft vulnerabilities CVE-20191462, CVE-2019-1485, CVE-2019-1476, CVE-2019-1478, CVE-2019-1483, CVE-2019-1458, and CVE-2019-1484, on Microsoft Windows Workstation and Server products.
2. Strictly monitor for any inbound or outbound communication on Port 9110.
3. Strictly restrict inbound communication on Ports 135, 139, 445, and 3389, from external networks (Internet).
4. Kindly restrict access on Ports 135, 139, 445, and 3389, for servers in production and access should only be granted when needed.
5. Ensure PowerShell and Remote Desktop features are Disabled on nonadministrative systems in production environment.
6. Ensure internet facing devices, applications and services are using strong & complex passwords.
7. Ensure proper access control and email filtering are in place to protect Email Exchange Servers and Email Accounts.
8. Ensure Web Applications are patched with latest security patches.
9. Ensure Web Application Firewall (WAF) is properly configured for deep inspection on web traffic.
10. Kindly Block mentioned IP/Domain on security devices.
11. Kindly Block Hashes, that are not detected by your Antivirus Program or not known to your Antivirus Vendor.

READ

Visa Warns of Point-of-Sale Attacks from FIN8 Hackers

HASHES (SHA-256)

Hashes	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
cc5b3904458b144c5f263f47a3dffc9628ecdccab993bf7e01d345f496692c1a	YES	YES	YES	NO	YES
3a934f3cea6f9aff894eafd6e25ed01a93ef7dc4f7a16e2ade2da9f12060908f	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
a7e41affb12e8e5c5e54cf9eb73104fb2069fb020eb2bf741f646f32b04d803a	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
431f83b1af8ab7754615adaef11f1d10201edfef4fc525811c2fcda7605b5f2e	NOT KNOWN	NOT KNOWN	YES	NO	NO

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Rancor, a Chinese-based Cyber Espionage Group found using customized malware and exploits, to target organizations in South-East Asia and other regions on global scale

Severity: High

Date: December 19, 2019

IP ADDRESSES

- 199.247.6.253
- 139.162.14.25

DOMAINS

- cswksfwq.kfesv.xyz
- Connect.bafunpda.xyz

TARGETED CVE

- CVE-2019-1458
- CVE-2019-1484
- CVE-2019-1485

REMEDIATION

1. Immediately apply Security Patches for Microsoft vulnerabilities CVE-20191485, CVE-2019-1458, and CVE-2019-1484, on Microsoft Windows Workstation and Server products.
2. Strictly monitor for any inbound or outbound communication on Port 9110.
3. Strictly restrict inbound communication on Ports 135, 139, 445, and 3389, from external networks (Internet).
4. Kindly restrict access on Ports 135, 139, 445, and 3389, for servers in production and access should only be granted when needed.
5. Ensure PowerShell and Remote Desktop features are Disabled on nonadministrative systems in production environment.
6. Ensure internet facing devices, applications and services are using strong & complex passwords.
7. Ensure proper access control and email filtering are in place to protect Email Exchange Servers and Email Accounts.
8. Ensure Web Applications are patched with latest security patches.
9. Ensure Web Application Firewall (WAF) is properly configured for deep inspection on web traffic.
10. Kindly Block mentioned IP/Domain on security devices.
11. Kindly Block Hashes, that are not detected by your Antivirus Program or not known to your Antivirus Vendor.

READ

Rancor: Cyber Espionage Group Uses New Custom Malware to Attack Southeast Asia

HASHES (SHA-256)

Hashes	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
0EB1D6541688B5C87F620E76219EC5DB8A6F05732E028A9EC36195D7B4F5E707	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
AAEBF987B8D80D71313C3C0F2C16D60874FFECBDDA3BB6B44D6CBA6D38031609	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
0D61D9BAAB9927BB484F3E60384FDB6A3709CA74BC6175AB16B220A68F2B349E	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
DB982B256843D8B6429AF24F766636BB0BF781B471922902D8DCF08D0C58511E	YES	NO	YES	NO	YES
CC081FFEA6F4769733AF9D0BAE0308CA0AE63667FA225E7965DF0884E96E2D2A	YES	YES	YES	YES	YES
BC1C3E754BE9F2175B718ABA62174A550CDC3D98AB9C36671A58073140381659	YES	NO	YES	NO	YES
83d1d181a6d583bca2f03c3c4e517757a766da5f4c1299fbbe514b3e2abd9e0d	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Ukraine-based Threat Actors found targeting organizations using sophisticated Carbanak Backdoor

Severity: Critical

Date: December 31, 2019

IP ADDRESSES

- 185.161.211.77
- 46.22.213.124
- 185.174.172.13
- 91.206.30.183
- 54.38.123.237
- 67.227.226.240
- 199.59.242.153
- 195.20.40.122

DOMAINS

- paraklit.com.ua
- xbabiessparty.com
- xadultclub.com
- welcometochicksparty.com
- yourhottestladies.com
- sweetkissparty.com
- prodexport.in.ua
- ttrcoin.com
- glasterius.tk
- agropromtehnica.com.ua
- gabaritkl.com.ua
- interier-plus.com
- luckagro.com.ua
- memorial-granite.com.ua
- olident.com.ua
- razom.com.ua
- virofex.com.ua
- yadobre.com.ua
- adultamusements.com
- advdll.com
- advkiss.com
- advlover.com
- allformacho.com
- babesallnight.com
- babesneedflirt.com
- babesneedfun.com
- babesneedkiss.com
- babesneedlove.com
- bestadultsfinder.com
- bestbabesfinder.com
- bestchicksfinder.com
- bestflingsfinder.com
- bestgirlsfinder.com
- bestladiesfinder.com
- bestloversfinder.com
- bestpartnersfinder.com
- bestplaymatesfinder.com
- bestprize4u.com
- bestslutsfinder.com
- betterwomens.com
- chicksallnight.com
- chicksneeddate.com
- chicksneedflirt.com
- chicksneedfun.com
- chicksneedkiss.com
- chicksneedlove.com
- datesweetcherrybabies.com
- datesweetcherrychicks.com
- datesweetcherrygirls.com
- datesweetcherryladies.com
- datesweetcherrylovers.com
- dreambabesfinder.com
- dreamchicksfinder.com
- dreamflingsfinder.com
- dreamgirlsfinder.com
- dreamslutsfinder.com
- fantastickluck.com
- fuckablelovers.com
- girlsallnight.com
- givebabeslove.com
- givegirlslove.com
- giveladieslove.com
- giveloverslove.com
- hereyourhotbabie.com
- hereyourhotchick.com
- hereyourhotgirl.com
- hereyourhotlady.com
- hereyourhotlover.com
- hereyourprettybabie.com
- hereyourprettyblady.com
- hereyourprettychick.com
- hereyourprettygirl.com
- hereyourprettylover.com
- hereyoursweetbabie.com
- hereyoursweetchick.com
- hereyoursweetgirl.com
- hereyoursweetlady.com
- hereyoursweetlover.com
- hottestsexybabies.com
- hottestsexychicks.com
- hottestsexydream.com
- hottestsexymilfs.com
- juicyadmirersfinder.com
- juicyadultsfinder.com
- juicybabesfinder.com
- juicyflingsfinder.com
- juicygirlsfinder.com
- juicyladiesfinder.com
- juicyloversfinder.com
- juicypartnersfinder.com
- juicyplaymatesfinder.com
- juicyslutsfinder.com
- ladiesallnight.com
- ladiesneeddate.com
- ladiesneedflirt.com
- ladiesneedfun.com
- ladiesneedkiss.com
- ladiesneedlove.com
- localdate69.com
- localhottestbabes.com
- localhottestchicks.com
- localhottestgirls.com
- localhottestladies.com
- localhottestlovers.com
- loversallnight.com
- meetsweetcherrylovers.com
- menbangclub.com
- menflirtclub.com
- menloveclub.com
- mensexclub.com
- perfectadultsfinder.com
- perfectbabesfinder.com
- perfectchicksfinder.com
- perfectflingsfinder.com
- perfectgirlsfinder.com

REMEDIATION

1. Ensure Microsoft Windows Workstations and Servers are up-to-date with latest security patches.
2. Strictly use least privilege accounts throughout the enterprise wide network.
3. Immediately apply Security Patches for Microsoft vulnerabilities CVE-20191478, CVE-2019-1458, CVE-2019-1408, CVE-2019-1394, CVE-2019-1393, CVE-2019-1396, CVE-2019-1395, CVE-2019-1362, CVE-2019-1364, CVE2019-1429, CVE-2019-1390, CVE-2019-1239, CVE-2019-1315, CVE-20191319, CVE-2019-1339, CVE-2019-1342, & CVE-2019-1333 on Windows OS.
4. Ensure to Disable SMB version 1 (SMBv1) on Windows OS.
5. Strictly restrict inbound communication on Ports 135, 139, 445, and 3389, from external networks (Internet).
6. Kindly restrict access on Ports 135, 139, 445, and 3389, for servers in production and access should only be granted when needed.
7. Ensure proper access control and email filtering are in place to protect Email Exchange Servers and Email Accounts.
8. Ensure PowerShell and Remote Desktop features are Disabled on nonadministrative systems in production environment.
9. Ensure internet facing devices, applications and services are using strong & complex passwords.
10. Kindly Block mentioned IP/Domain on security devices.
11. Kindly Block Hashes, that are not detected by your Antivirus Program or not known to your Antivirus Vendor.

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Ukraine-based Threat Actors found targeting organizations using sophisticated Carbanak Backdoor

Severity: Critical

Date: December 31, 2019

- perfectladiesfinder.com
- perfectloversfinder.com
- perfectpartnersfinder.com
- perfectplaymatesfinder.com
- perfectslutsfinder.com
- prettychicksfordate.com
- prettychicksforkisses.com
- prettygirlsfordate.com
- prettygirlsforkisses.com
- prettyladiesfordate.com
- prettyloversforkisses.com
- prettysweetgirlsonly.com
- raspberryxfantasy.com
- raspberryxladies.com
- raspberryxlovers.com
- secretdate1.com
- snapchicks.com
- sweetadultclub.com
- sweetadultparty.com
- sweetbabiesparty.com
- sweetchicksclub.com
- sweetgirlsparty.com
- sweetkissesclub.com
- sweetladiesparty.com
- sweetloversclub.com
- sweetsexx.com
- sweetxbabies.com
- sweetxladies.com
- sweetxxxfantasy.com
- sweetxxxparty.com
- tophotbabies.com
- tophotchicks.com
- tophotladies.com
- tophotlovers.com
- topxchicks.com
- topxladies.com
- topxlovers.com
- topxmilfs.com
- trkmil.com
- trkwaz.com
- trkwdd.com
- trkwht.com
- trkwov.com
- trkwrs.com
- unlimitedbabesfinder.com
- unlimitedchicksfinder.com
- unlimitedflingsfinder.com
- unlimitedgirlsfinder.com
- unlimitedslutsfinder.com
- urlovelybabes.com
- urlovelychicks.com
- urlovelygirls.com
- urlovelylovers.com
- urlovelyvalentine.com
- welcometoadultparty.com
- welcometoladiesparty.com
- xadultdream.com
- xadultfantasy.com
- xadultparty.com
- xchickssparty.com
- xxxxfantasy.com
- xxxxfriends.com
- youareluckyone.com
- yourloveamusement.com
- yourmatureamusement.com
- yourpieceofluck.com
- yourtodayreward.com

READ

Introducing BIOLOAD: FIN7 BOOSTWRITE's Lost Twin

HASHES (SHA-256)

Hashes	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
7bdae0dfc37cb5561a89a0b337b180ac6a139250bd5247292f470830bd96dda7	YES	YES	YES	NO	YES
c1c68454e82d79e75fefad33e5acbb496bbc3f5056dfa26aaf1f142cee1af372	YES	YES	YES	NO	YES
77a6fbd4799a8468004f49f5929352336f131ad83c92484b052a2eb120ebaf9a	YES	YES	YES	NO	YES
42d3cf75497a724e9a9323855e0051971816915fc7eb9f0426b5a23115a3bdcb	YES	YES	YES	NO	YES
b6bbb6035e1ee52d8a5fb0c3dd79a4a04dc69a63ad49b05d30f2238bbb0bdcd7	NO	NO	YES	NO	NO
230accadbfb73bf7fc78d4dfdb74a20b829d8f830a4fd829c088494b74bee779	NO	NOT KNOWN	YES	NO	NO
983a67229acb226223da37ea80ab329d996c384ff83fb047ec6427eb622c4738	NO	NO	NO	NO	NO

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

An exploitable Remote Code Execution vulnerability (CVE-201910758) found in MongoDB Mongo-Express, which can allow a remote attacker to execute arbitrary code on the affected system

Severity: Critical

Date: January 06, 2020

IMPACT

This Dexphot Malware poses a serious risk of disruption of business application or/and operation.

EXPLOITABLE CVE IDs

CVE-2019-10758

VULNERABLE

1. Kindly upgrade MongoDB MongoExpress to version 0.54.0 or higher.

2. Ensure any Database linked to the MongoDB Mongo-Express, are timely backed-up in isolated environment (as part of Disaster Recovery Plan for Ransomware attack).

3. Ensure proper file permission and access controls are in place, to secure MongoDB Mongo-Express instances from unauthorized access and data breach

INTRODUCTION

An exploitable Remote Code Execution vulnerability (CVE-2019-10758) found in MongoDB Mongo-Express (a lightweight web-based administrative interface deployed to manage MongoDB databases interactively), which can allow a remote attacker to execute arbitrary code on the affected system.

The MongoDB Mongo-Express versions prior to 0.54.0 are exploitable via endpoints that uses the `toBSON` method, which as a result allow remote attacker to misuse the `vm` dependency to perform `exec` commands in a non-safe environment.

The Remote Code Execution vulnerability (CVE-2019-10758) in MongoDB Mongo-Express poses a serious risk of unauthorized access to and data breach of any linked Database Management System. This vulnerability can also be exploited by remote attacker in favor of executing successful Ransomware attack against the Database Management System or Database files on affected systems.

AFFECTED PRODUCTS

Systems running MongoDB Mongo-Express versions prior to 0.54.0, are vulnerable to Hack and Ransomware attacks

READ

- MongoDB Mongo-Express | CVE-2019-10758
- MongoDB mongo-express Remote Code Execution (CVE-201910758)

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

16th December 2019 – 22nd December 2019 | TRAC-ID: NII19.12.0.4

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
December 19, 2019	Ubuntu Linux	USN-4224-1: Django vulnerability	▪ Ubuntu 19.10 ▪ Ubuntu 19.04 ▪ Ubuntu 18.04 LTS ▪ Ubuntu 16.04 LTS	Follow Update instructions
December 17, 2019	Ubuntu Linux	USN-4223-1: OpenJDK vulnerabilities	▪ Ubuntu 19.10 ▪ Ubuntu 19.04 ▪ Ubuntu 18.04 LTS ▪ Ubuntu 16.04 LTS	Follow Update instructions
December 16, 2019	Ubuntu Linux	USN-4222-1: GraphicsMagick vulnerabilities	▪ Ubuntu 16.04 LTS	Follow Update instructions

REDHAT

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
December 19, 2019	Red Hat JBoss Middleware	RHSA-2019:4352	▪ Red Hat JBoss Middleware Text-Only Advisories for MIDDLEWARE 1 x86_64	Security Patch Update
December 19, 2019	Red Hat Enterprise Linux	RHSA-2019:4326	▪ Red Hat Enterprise Linux Server 7 x86_64 ▪ Red Hat Enterprise Linux for x86_64 - Extended Update Support 7.7 x86_64 ▪ Red Hat Enterprise Linux Server - AUS 7.7 x86_64 ▪ Red Hat Enterprise Linux Workstation 7 x86_64 ▪ Red Hat Enterprise Linux Desktop 7 x86_64 ▪ Red Hat Enterprise Linux EUS Compute Node 7.7 x86_64 ▪ Red Hat Enterprise Linux Server - TUS 7.7 x86_64	Security Patch Update

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

REDHAT

December 16, 2019	Red Hat Enterprise Linux	RHSA-2019:4240	▪ Red Hat Enterprise Linux Server 7 x86_64 ▪ Red Hat Enterprise Linux for x86_64 - Extended Update Support 7.7 x86_64 ▪ Red Hat Enterprise Linux Server - AUS 7.7 x86_64 ▪ Red Hat Enterprise Linux Workstation 7 x86_64 ▪ Red Hat Enterprise Linux Desktop 7 x86_64 ▪ Red Hat Enterprise Linux EUS Compute Node 7.7 x86_64 ▪ Red Hat Enterprise Linux Server - TUS 7.7 x86_64	Security Patch Update
December 16, 2019	Red Hat Enterprise Linux	RHSA-2019:4238	▪ Red Hat Enterprise Linux Server 6 x86_64 ▪ Red Hat Enterprise Linux Server 6 i386 ▪ Red Hat Enterprise Linux Workstation 6 x86_64 ▪ Red Hat Enterprise Linux Workstation 6 i386 ▪ Red Hat Enterprise Linux Desktop 6 x86_64 ▪ Red Hat Enterprise Linux Desktop 6 i386	Security Patch Update

SUSE

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
December 21, 2019	SUSE Linux	Security update for the Linux Kernel	▪ SUSE Linux Enterprise Server for SAP 12-SP3 ▪ SUSE Linux Enterprise Server 12-SP3-LTSS ▪ SUSE Linux Enterprise Server 12-SP3-BCL ▪ SUSE Linux Enterprise High Availability 12-SP3	Security Patch Update
December 20, 2019	SUSE Linux	Security update for MozillaFirefox, mozilla-nspr, mozilla-nss	▪ SUSE Linux Enterprise Server 11-SP4-LTSS	Security Patch Update
December 19, 2019	SUSE Linux	Security update for the Linux Kernel	▪ SUSE Linux Enterprise Module for Public Cloud 15-SP1	Security Patch Update