NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

August 2020, Edition 2.0

NETWORK INTELLIGENCE SECURITY ADVISORY

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

IN THIS EDITION:

Security Advisory Listing	Severity
Threat Actors found targeting Banking & Financial Institutions, and FinTech Organizations by luring as COVID-19 protective equipment company.	High
One of the unnamed subsidiary owned by Carnival Corporation suffered data breach followed by security breach incident.	Critical
Threat Actors behind Operation PowerFall found using Zero-Day Exploits to target vulnerabilities in Internet Explorer and Windows OS.	Critical
A chinese-based APT Threat Actors called CactusPete found targeting Government & Defense, and Banking & Financial Institutions using new variant of Bisonal backdoor.	Critical

ALSO INSIDE

Data Breach Highlights

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

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Threat Actors found targeting Banking & Financial Institutions, and FinTech Organizations by luring as COVID-19 protective equipment company.

Severity: High

Date: August 26, 2020

IP ADDRESSES

82.239.200.118
51.255.15.193
185.81.158.15
85.25.207.108
74.109.108.202
192.185.5.43
154.219.173.66
178.210.75.228
13.232.244.117
88.249.181.198
185.86.148.68
189.39.32.161
107.161.30.122
113.161.148.81
74.208.173.91
139.59.12.63
188.0.135.237
2.144.244.204
87.106.231.60
181.137.229.1
173.94.215.84
175.29.183.2
37.46.129.215
86.57.216.23
181.126.54.234
190.212.140.6
46.105.131.68
190.190.15.20
139.99.157.213
168.0.97.6
217.199.160.224
185.142.236.163
220.254.198.228
202.5.47.71
188.251.213.180
198.57.203.63
190.55.186.229
37.187.100.220
86.98.143.163
157.7.164.178
195.201.56.70
5.79.70.250
91.83.93.103
41.185.29.128
105.209.235.113
190.53.144.120
192.163.221.191
115.78.11.155
177.32.8.85
192.210.217.94
71.57.180.213
179.5.118.12
66.61.94.36
31.146.61.34
162.249.220.190
177.144.130.105
51.38.201.19
197.221.158.162
77.74.78.80
179.62.238.49
185.208.226.142
177.94.227.143
81.214.253.80
78.189.60.109
50.116.78.109
181.113.229.139
60.125.114.64
178.33.167.120
190.164.75.175
75.127.14.170
143.95.101.72
81.17.93.134
192.241.220.183
45.182.161.17
172.105.78.244
115.79.195.246
172.96.190.154
113.203.250.121
37.210.226.93
46.32.229.152
201.213.177.139
95.216.205.155
203.153.216.178
201.235.10.215

DOMAINS

cryptokuota.com
luxelistreviews.com
yhyhzx.com
mediadrive.nichost.ru
kumarpratham.com
fxea.club
xiangfu.phjrt.com
batamry.com

EMAILS

smstmed1<@>emirates.net.ae
ptasihuano<@>automundial.co

REMEDIATION

1. Immediately apply Security Patches for Microsoft vulnerabilities CVE-2020-1380, CVE-2020-1464, CVE-2020-1472, CVE-2020-1519, CVE-2020-1538, CVE-2020-1579, CVE-2020-1337, CVE-2020-0986, CVE-2020-0674, CVE- 2019-1429, CVE-2019-0676, & CVE-2018-8653 on Microsoft Windows Workstation and Server.

2. Ensure Microsoft Windows Workstation and Server are patched with latest security updates.

3. Ensure Domain Accounts follows least privilege principle and ensure TwoFactor authentication is enabled on all Business Email Accounts.

4. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through VPN tunnel
.
5. Ensure VPN client software and VPN servers are patched with latest security updates released by vendor.

6. Strictly ensure TCP Port 135, TCP Port 445, and TCP Port 3389 are not left open on Internet or DMZ facing side.

7. Please ensure TCP Port 135 (Remote Procedure Call - RPC), TCP Port 445 (Server Message Block - SMB), and TCP Port 3389 (Remote Desktop Protocol-RDP) are only accessible through VPN tunnel between VPN clients and Organization's Resources.

8. Ensure proper network segmentation are done, and ensure communication through TCP Port 135, TCP Port 445, and TCP Port 3389 are explicitly allowed on-demand only for particular network segments when needed.

9. Ensure network segments that allows communication over TCP Port 135, TCP Port 445, and TCP Port 3389 are strictly monitored for any anomaly or suspicious patterns like lateral movement, excessive network traffics on TCP Port 135, TCP Port 445, TCP Port 3389, and unusual amount of data transmission, etc.

10. Ensure VNC, SOCKS, and SMTP ports are also closely monitored.

11. Ensure data backup is done periodically and ensure data backups are done via out-of-band network onto the server with limited or no internet access.

12. Kindly Block IPs and Domains on the perimeter security devices.

13. Kindly Block Hashes, that are not detected by your Antivirus Program or not known to your Antivirus Vendor

URLS

http<://www>.cryptokuota.com/assets/ayQUtnd403/
http<://www>.luxelistreviews.com/wp-includes/AYR/
https<://www>.yhyhzx.com/wp-admin/pKpz/
http<://>mediadrive.nichost.ru/awfcatfre/9thw57489/
http<://>kumarpratham.com/fonts/Wtuq/
http<://>fxea.club/wp-includes/mPqJMPzx/
https<://>xiangfu.phjrt.com/0qeoy/voB355f13v2j475/
https<://www>.batamry.com/tmp/baeng79095371/
http<://>82.239.200.118/4LfrF/F2URscLIbJtolRG8v/
http<://>85.25.207.108:8080/GBIy5HqLanoQdJAhT/Il4VMycB1/
http<://>185.81.158.15:8080/WGxaSdsxEfhBB/YhYXU/z8sh70b6WQ9XXx/HpSlucg/1w9Qtfvyg9G/h4QArc7EuwBBT/
http<://>74.109.108.202/CS2rWWpxy/l9DBs2Bf/qUdCuB/TyXwKD/
http<://>74.109.108.202/CS2rWWpxy/l9DBs2Bf/qUdCuB/TyXwKD/X
http<://>74.109.108.202/R1ZwTA8q9GhtcY/Wqn5tZjXWELFGUARgK2/ipEUD5NO7i/
http<://>74.109.108.202/bgQFoe8NrzjU8/evFzwPZK4cNYDmVQmU/9D1ybWiFoWUVz6/ZyT7/U0PWyq2WQl81xX/Ui5z/

READ

- Emotet malware spreading under the guise of a Corona 19 protective equipment company

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Threat Actors found targeting Banking & Financial Institutions, and FinTech Organizations by luring as COVID-19 protective equipment company.

Severity: High

Date: August 26, 2020

HASHES (SHA-256)

HASHES	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
9811fc7224ac578359229ed16dfd3d799a3e667abfaa33174358809d588d04ec	Yes	Yes	Yes	No	No
2065fa92812ddff0bca8ab3fc907dbfc5048e36f8d20bc0acdf0b8d3d9cd82c8	Yes	No	Yes	No	Yes
8b937281f6ef74d57ac4527564b451c45e6293e42fa53a96bc34a74a8d54ccd7	Yes	No	Yes	No	Yes
cd150a7cdaeb8b2d9c02a8d509c8463400e40f8aa52a31dc4ef7d4d184d7e699	No	No	No	No	Yes
6E780F1D204CCF0208399546D785B5B82988C237888BB3C84F98D67B4C46D43A	Not Known	Not Known	Not Known	Not Known	Not Known
3D701B314396DBC47ADD3D0180D09B7F2D705FB11EE29CD8222438C6D779F5C1	Not Known	Not Known	Not Known	Not Known	Not Known
e18f7b9ab4d955451e48b87b52d24a29ec813df7cbc7ace9706738bebd2b6181	Yes	Yes	Yes	No	No
8287c0ee920f91527cec78ed8534470c69ed84d14b8c4c25b96b44f9b89e5b4a	No	No	Yes	No	No
4EC465D311921B9264539B05D3B1A9319C9876C0BE632E2CBF617A781319B8E2	Not Known	Not Known	Not Known	Not Known	Not Known

HASHES (MD5)

HASHES	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
feaab7f361af7eb0211cb93939ecaab	Not Known	Not Known	Not Known	Not Known	Not Known

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

One of the unnamed subsidiary owned by Carnival Corporation suffered data breach followed by security breach incident

Severity: Critical

Date: August 20, 2020

RECOMMENDATION

1. Ensure Amazon Web Service (Amazon EC2, Amazon ELB, Amazon CloudFront, Amazon RDS, and Amazon S3 Bucket) follows best security practices and access controls are timely reviewed.

2. Ensure Apache HTTP or Apache Tomcat web server hosted on Amazon EC2 is running latest release, and timely assessed for vulnerability & misconfiguration issues.

3. Ensure Remote Desktop (RDP), Remote Procedure Call (RPC), and Virtual Network Computing (VNC) Services are strictly isolated from internet facing cloud or onpremise IT infrastructure. And ensure these remote services are only allowed through VPN tunnels.

4. Ensure vulnerable SMB protocols, are strictly disabled from internet facing cloud or on-premise IT infrastructure. And ensure SMB must be used in controlled environment, and only be used when filesharing is required.

5. Ensure network segmentation is done properly and ensure sensitive data hosting servers are completely isolated from other networks or systems.

6. Ensure to closely monitor for any intrusion or suspicious activities on the system and network, via SIEM solution throughmanaged SOC service.

7. Procure services to detect Personally Identifiable Information (PII) over Internet and Darkweb related to your organization/brand.

INTRODUCTION

One of the unnamed subsidiary owned by Carnival Corporation suffered data breach followed by security breach incident.

The incident took place on August 15, 2020 where attacker had unauthorized access onto the system associated with unnamed subsidiary owned by Carnival Corporation and downloaded personal data of customers and employees prior to executing Ransomware attack.

Carnival Corporation did not reveal any additional information such as name of the affected subsidiary and name of the ransomware used in the attack.

However, our Threat Intelligence Team at Network Intelligence (I) Pvt. Ltd., did their Threat Intelligence Analysis to determine further information relevant to this incident, and their analysis reveals that,

AIDA Cruises (a German Branch of Costa Crociere S.p.A.) which is a subsidiary owned by Carnival Corporation, is a suspected victim of the Sodinokibi Ransomware attack took place on August 15, 2020.

The Ransomware operator behind the attack gained unauthorized access onto the Apache web server hosting Single Sign-On application for customers andemployees, and executed Sodinokibi Ransomware attack on the Apache web server and other servers within same Availability Zone (IP subnet) as configured in Amazon Elastic Load Balancing (ELB) within Amazon AWS Cloud Environment.

Our Threat Intelligence Team further added that, the incident appears to be the result of misconfiguration issue in Amazon Elastic Load Balancing (ELB), and use of vulnerable or misconfigured Apache web server that gave Ransomware operator limited access on few servers (in same IP subnet) within Amazon AWS cloud environment.

LESSON LEARNED

- Misconfiguration issues and use of vulnerable or misconfigured software in Amazon AWS cloud, often allows remote attackers to gain initial footholds onto Amazon AWS cloud environment and unauthorized access onto the sensitive data hosted on connected servers.

- Lack of network segmentation gives attacker a wider access onto the entire Amazon AWS cloud environment, which prevents organization from containing the damage caused by attackers.

- Failed to limit the exposure of the services hosted on Amazon AWS cloud environment, would allow remote attackers to gather technical details on Amazon AWS cloud, and well plan their attack.

READ

- Carnival Corporation Discloses Ransomware Attack; Personal Data of Employees and Guests Potentially Accessed

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Threat Actors behind Operation PowerFall found using Zero-Day Exploits to target vulnerabilities in Internet Explorer and Windows OS.

Severity: Critical

Date: August 18, 2020

IP ADDRESSES

139.180.210.149

DOMAINS

static-cdn1.com
kxsw.club
wtb.kxsw.club
thyaokanwangjian.website
yt.thyaokanwangjian.website

URL

http<://www>.static-cdn1.com/update.zip

REMEDIATION

1. Immediately apply Security Patches for Microsoft vulnerabilities CVE-2020-1380, CVE-2020-1464, CVE-2020-1472, CVE-2020-1519, CVE-2020-1538, CVE-2020-1579, CVE-2020-1337, CVE-2020-0986, CVE-2020-0674, CVE- 2019-1429, CVE-2019-0676, & CVE-2018-8653 on Microsoft Windows Workstation and Server.

2. Ensure Microsoft Windows Workstation and Server are patched with latest security updates.

3. Ensure Domain Accounts follows least privilege principle and ensure TwoFactor authentication is enabled on all Business Email Accounts.

4. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through VPN tunnel.

5. Ensure VPN client software and VPN servers are patched with latest security updates released by vendor.

6. Strictly ensure TCP Port 135, TCP Port 445, and TCP Port 3389 are not left open on Internet or DMZ facing side.

7. Please ensure TCP Port 135 (Remote Procedure Call - RPC), TCP Port 445 (Server Message Block - SMB), and TCP Port 3389 (Remote Desktop Protocol-RDP) are only accessible through VPN tunnel between VPN clients and Organization's Resources.

8. Ensure proper network segmentation are done, and ensure communication through TCP Port 135, TCP Port 445, and TCP Port 3389 are explicitly allowed on-demand only for particular network segments when needed.

9. Ensure network segments that allows communication over TCP Port 135, TCP Port 445, and TCP Port 3389 are strictly monitored for any anomaly or suspicious patterns like lateral movement, excessive network traffics on TCP Port 135, TCP Port 445, TCP Port 3389, and unusual amount of data transmission, etc.

10. Ensure VNC, SOCKS, and SMTP ports are also closely monitored.

11. Ensure data backup is done periodically and ensure data backups are done via out-of-band network onto the server with limited or no internet access.

12. Kindly Block IPs and Domains on the perimeter security devices.

13. Kindly Block Hashes, that are not detected by your Antivirus Program or not known to your Antivirus Vendor.

READ

- Internet Explorer and Windows zero-day exploits used in Operation PowerFall

HASHES (SHA-256)

HASHES	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
D02632CFFC18194107CC5BF76AECA7E 87E9082FED64A535722AD4502A4D51199	Not Known	Not Known	Not Known	Not Known	Not Known
7577E42177ED7FC811DE4BC854EC226EB 037F797C3B114E163940A86FD8B078B	Not Known	Not Known	Not Known	Not Known	Not Known
7765F836D2D049127A25376165B1AC43C D109D8B9D8C5396B8DA91ADC61ECCB1	Not Known	Not Known	Not Known	Not Known	Not Known
81D07CAE45CAF27CBB9A1717B08B3AB3 58B647397F08A6F9C7652D00DBF2AE24	Not Known	Not Known	Not Known	Not Known	Not Known

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

A chinese-based APT Threat Actors called CactusPete found targeting Government & Defense, and Banking & Financial Institutions using new variant of Bisonal backdoor

Severity: Critical

Date: August 18, 2020

REMEDIATION

1. Immediately apply Security Patches for Microsoft vulnerabilities CVE-2020-1380, CVE-2020-1464, CVE-2020-1472, CVE-2020-1519, CVE-2020-1538, CVE-2020-1579, & CVE-2020-1337 on Microsoft Windows Workstation and Server.

2. Ensure Domain Accounts follows least privilege principle and ensure Two-Factor authentication is enabled on all Business Email Accounts.

3. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through VPN tunnel
.
4. Ensure VPN client software and VPN servers are patched with latest security updates released by vendor.

5. Strictly ensure TCP Port 135, TCP Port 445, and TCP Port 3389 are not left open on Internet or DMZ facing side.

6. Please ensure TCP Port 135 (Remote Procedure Call - RPC), TCP Port 445 (Server Message Block - SMB), and TCP Port 3389 (Remote Desktop Protocol - RDP) are only accessible through VPN tunnel between VPN clients and Organization's Resources.

7. Ensure proper network segmentation are done, and ensure communication through TCP Port 135, TCP Port 445, and TCP Port 3389 are explicitly allowed on-demand only for particular network segments when needed.

8. Ensure network segments that allows communication over TCP Port 135, TCP Port 445, and TCP Port 3389 are strictly monitored for any anomaly or suspicious patterns like lateral movement, excessive network traffics on TCP Port 135, TCP Port 445, TCP Port 3389, and unusual amount of data transmission, etc.

9. Ensure VNC, SOCKS, and SMTP ports are also closely monitored.

10. Ensure data backup is done periodically and ensure data backups are done via out-of-band network onto the server with limited or no internet access.

11. Kindly Block Hashes, that are not detected by your Antivirus Program or not known to your Antivirus Vendor.

READ

- CactusPete APT group’s updated Bisonal backdoor

HASHES (MD5)

HASHES	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
A3F6818CE791A836F54708F5FB9935F3	Not Known	Not Known	Not Known	Not Known	Not Known
3E431E5CF4DA9CAE83C467BC1AE818A0	Not Known	Not Known	Not Known	Not Known	Not Known
11B8016045A861BE0518C9C398A79573	Not Known	Not Known	Not Known	Not Known	Not Known

NETWORK INTELLIGENCE
Global cybersecurity provider

NEWSLETTER

August 2020, Edition 2.0

DATA BREACH HIGHLIGHTS

Dave Inc., a Digital Banking service suffered security breach followed by data breach incident caused by a threat actor called ShinyHunters

July 28, 2020

- Tech unicorn Dave admits to security breach impacting 7.5 million users
- Hacker leaks 386 million user records from 18 companies for free
- Digital banking app Dave.com discloses a security breach after the known threat actor ShinyHunters leaked 7 million user records on a crime forum

Dussmann group, the German largest multi-service provider suffered security breach followed by data breach incident caused by Nefilim ransomware operators

July 28, 2020

- NEFILIM RANSOMWARE OPERATORS ALLEGEDLY TARGETED THE DUSSMANN GROUP, GERMANY'S LARGEST PRIVATE MULTI-SERVICE PROVIDER
- Nefilim ransomware operators leaked data alleged stolen from the Dussmann group

Orange Business Services, a subsidiary of Orange S.A,suffered security breach followed by data breach incident caused by Nefilim ransomware operators

July 17, 2020

- Orange confirms ransomware attack exposing business customers' data
- Orange, Europe's Fourth-Largest Mobile Operator, Confirms Ransomware Attack
- Orange Business Services hit by Nefilim ransomware operators