



On March 16, the [Cyber Threat Alert Level](#) was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Adobe, PTC, Schneider, Veeam, Apple, and Google products. [CIS Advisories](#)

#### Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
18 Mar 22	466,688,644	6,089,257

Deaths this week: 37,067

## WEEKLY IT SECURITY BULLETIN

### 18 March 2022

### In The News This Week

#### Biden's cryptocurrency executive order addresses illicit financial risks

Early indications are that the cryptocurrency industry will work with the U.S. government to help minimize risk and make it harder for cybercriminals to profit from their activities. - The Biden administration issued its much-anticipated cryptocurrency executive order, laying out a wide-ranging investigation into digital assets to gain at least a preliminary grasp on how to address the rapidly growing \$3 trillion financial market and its role in ransomware and other illicit activities. The order, entitled "[Ensuring Responsible Development of Digital Assets](#)", outlines a series of far-reaching goals, including reducing the risks that digital assets could pose to consumers and investors, improving business protections, financial stability, and financial system integrity, combating and preventing crime and illicit finance, enhancing national security, fostering human rights and financial inclusion, and addressing climate change and pollution. [Read the rest of the story by Cynthia Brumfield here: CSO](#)

#### South Africa - Credit bureau TransUnion hacked – ransom sought

One of South Africa's largest credit bureaus, TransUnion, has been hacked. The company said in a statement on Friday that a third party obtained access to one of its servers through "misuse of an authorised client's credentials". "We have received an extortion demand and it will not be paid," the company said. "Immediately upon discovery of the incident, TransUnion South Africa suspended the client's access, engaged cybersecurity and forensic experts, and launched an investigation," it added. It said that it took "certain" of its services offline as a precautionary measure, but these services are now back online. "We believe the incident impacted an isolated server holding limited data from our South African business. We are working with law enforcement and regulators," the company said. ITWeb reported that the attackers, known as the Brazilian hacker group N4ughtysecTU, were demanding US\$15-million (R224-million) in ransom within seven days and that they had stolen 4TB of data from TransUnion made up of the personal records of 54 million South Africans.... [Read the rest of the story here: TechCentral](#)

#### New Variant of Russian Cyclops Blink Botnet Targeting ASUS Routers

ASUS routers have emerged as the target of a nascent botnet called Cyclops Blink, almost a month after it was revealed the malware abused WatchGuard firewall appliances as a stepping stone to gain remote access to breached networks. According to a new report published by Trend Micro, the botnet's "main purpose is to build an infrastructure for further attacks on high-value targets," given that none of the infected hosts "belong to critical organizations, or those that have an evident value on economic, political, or military espionage." Intelligence agencies from the U.K. and the U.S. have characterized Cyclops Blink as a replacement framework for VPNFilter, another malware that has exploited network devices, primarily small office/home office (SOHO) routers, and network-attached storage (NAS) devices. [Read the rest of the article here: The Hacker News](#)

#### VPNs Give Russians an End Run Around Censorship

As the invasion of Ukraine continues, Russian citizens have turned to virtual private networks to circumvent the government's blocks on social media and news sites critical of the war. - Russian citizens seeking to continue using social media sites and accessing international news have caused the demand for virtual private network (VPN) services to spike by a factor of 27 on Monday and a factor of 16 on Tuesday, compared to the daily average in February, according to industry sources. In early March, the Russian government severely limited the bandwidth of systems trying to access several social media services, including Facebook and Instagram, labelling the networks' parent company Meta an extremist organization for allowing calls of violence against the Russian government on the platforms. On March 11, Russia announced it would completely block Instagram. Provider Atlas VPN saw a wave of new installations beginning on March 11, when the Russian government announced its decision to block Instagram. The surge peaked on March 14 with increase in installations of its product that reached 110 times the normal amount, says spokesman Edvardad Garbenis.... Governments that seek to enforce censorship find themselves in a cat-and-mouse game with international providers, says Atlas VPN's Garbenis. China, for example, puts a great deal of effort into blocking VPNs, but the major providers typically find ways around the technical outages.... [Read more here: Dark reading](#)

For Reporting Cyber Crime in the USA go to the [Internet Crime Complaint Center \(IC3\)](#)

What do you mean, "there is no chips"?



### Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

### Chip shortage update

In October last year, I reported on the global short supply of semiconductor chips (silicon microchips) that literally makes our electronic world go round. And this week the shortage was highlighted again as several auto manufacturers announced production cuts and some are even rolling out models with omitted features that will be added once manufacturing can catch up. But it is not only the automotive industry that's impacted, it is the manufacturing of anything electronic including phones, computers, surveillance & security systems, household appliances, robotics, and other automation initiatives. In other words, most of the things that make our modern world function are reliant on semiconductors in some way or another. It is in nearly everything with a computing component and basically, if it has a screen, it has one or more semiconductor chips inside. It is a supply chain issue and at the moment, manufacturers need more of these chips than the chipmakers can make.

Why is there a shortage in the first place? - Most of the global manufacturing capacity for semiconductors is located in Asia, which was the first region to shut down at the beginning of the COVID-19 pandemic in 2020. Some of these factories were offline for months. Semiconductors are incredibly complex, and they take a long time to make, in the neighbourhood of three months, start to finish. So, when a plant shut down for a month, the first chips will only roll out 4 months after the shutdown commenced.

When the powers to be in the Western world realized that they became extensively dependent on the Asian region for semiconductor chips, large organizations like Intel and the like, adopted a globalization strategy to establish manufacturing plants in other parts of the world to ensure a steady supply. This is to say, a steady supply that can weather the impact of pandemics, civil unrest, and even the current Russian invasion of the Ukraine which had a massive impact on supply chains.

Building a new semiconductor manufacturing plant however, is not as simple as it sounds, and can take anything from three to five years to complete. Although the raw materials needed like neon, palladium, silica etc., are normally in [abundant supply](#) all around the globe, world events like the pandemic and the current Russian invasion of Ukraine can also hamper the supply of these materials which will influence the decision of where to establish new plants.

With that being said, below then are some of the recent headlines that will give you some insight into the overall global chip situation.

#### Toyota forced to make deeper production cuts due to chip shortage

Toyota Motor will make additional production cuts in March due to a shortage of semiconductor chips, days after the automaker reduced its domestic production target by as much as 20 percent for the April-June quarter. Toyota on Tuesday said it would suspend production on one line at a factory for eight weekdays starting March 22 through the end of the month. That is in addition to the suspension of domestic production at two factories announced last month... [Read more here: Automotive News](#)

#### The Global Fight Over Chips Is About to Get Even Worse

Sanctions are causing a shortage of microchips in Russia. Meanwhile, the U.S. and Europe are spending billions in a race with China that could easily backfire. - Magdeburg in former East Germany is famous for its towering gothic cathedral, and not a lot else. It's now about to play a key role in U.S. and European efforts to tilt the global balance of power. Intel Corp. unveiled plans on March 15 to build a giant, 17 billion-euro (\$18.7 billion) factory making cutting-edge semiconductors in the city, adding to new plants in Arizona and Ohio the company announced over the past six months. They are part of Chief Executive Officer Pat Gelsinger's plan to wrest control of production from Asia and tackle the global shortage of chips exacerbated during the Covid-19 pandemic and exposed again following Russia's invasion of Ukraine.... [Read the rest of the article here: Bloomberg](#)

#### Ford Plans To Ship Cars That Are Missing Features To Dealers Because Of The Chip Shortage

The company said that the missing features will be installed in the vehicles within a year. - Ford is facing a crisis. Like all automakers, it's a problem on dual fronts: on one hand, there are inventory-starved dealers who need vehicles to sell, and on the other, there are parking lots with vehicles piling up that aren't finished because of the lack of computer chips. Things have gotten so desperate that, as Automotive News reports, Ford is just saying "screw it," choosing to ship and sell these unfinished vehicles and install the missing features at a later date.... [Read more here: Jalopnik](#)

#### Here's how bad the chip shortage is, according to the White House

Today, the White House is saying out loud what you've likely already heard: the chip shortage won't end anytime soon. "We aren't even close to being out of the woods," said US Commerce Secretary Gina Raimondo in a briefing with reporters today, according to [Bloomberg](#), [The Washington Post](#), and others. Her comments come alongside a new Department of Commerce report that cites chipmakers who "did not see the problem going away in six months," which also isn't exactly news: chipmakers like Nvidia and AMD have repeatedly suggested the shortage wouldn't ease until the second half of 2022, while [Intel has said](#) it might not end until 2023... "The semiconductor supply chain remains fragile, and it is essential that Congress pass chips funding as soon as possible," reads a [statement from Raimondo](#).... [Read more here: The Verge](#)

#### U.S. Department of Commerce Report - Results from Semiconductor Supply Chain Request for Information - ...

Utilization: Since the semiconductor shortage started in 2020, semiconductor companies have significantly increased the utilization of their existing capacity. Specifically, from Q2 of 2020 through 2021, semiconductor fabs operated at over 90% utilization, which is incredibly high for a production process that requires regular maintenance and very high amounts of energy.... [Read the rest of the report here: U.S. Department of Commerce](#)

### Other Interesting News and Cyber Security bits:

- ❖ [Multiple Automotive Manufacturers Infected With Emotet](#)
- ❖ [Would 'Cyber Geneva Conventions' Defuse Online Aggression?](#)
- ❖ [Ukraine satellite images show extensive damage from Russian attacks](#)
- ❖ [SANS Daily Network Security Podcast \(Storm cast\)](#)



**AUTHOR: CHRIS BESTER** (CISA,CISM)  
chris.bester@yahoo.com

#### World's Worst Spam Support ISP's

Source <https://www.spamhaus.org/statistics/networks/>

