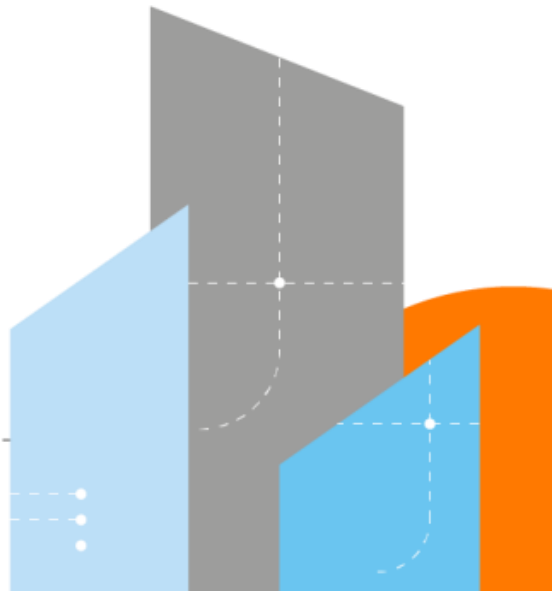
Orange
Cyberdefense

Security Intelligence

Monthly Report

April 2022



CONTENTS

INTRODUCTION

This is the first report we have published since the Signals service was officially deprecated and migrated to the World Watch service. This is definitely a step in the right direction, ensuring that the same standard service is being delivered to all Orange Cyberdefense customers, however unfortunately it does have an impact on the data used in this report.

Due to the different methodologies and systems used to deliver the World Watch service, for the time being we do not have access to the data required to produce the statistics and charts we would normally provide. With this in mind, a number of sections will now be deprecated, and we will work to reinvent the report going forward with new, useful and relevant content.

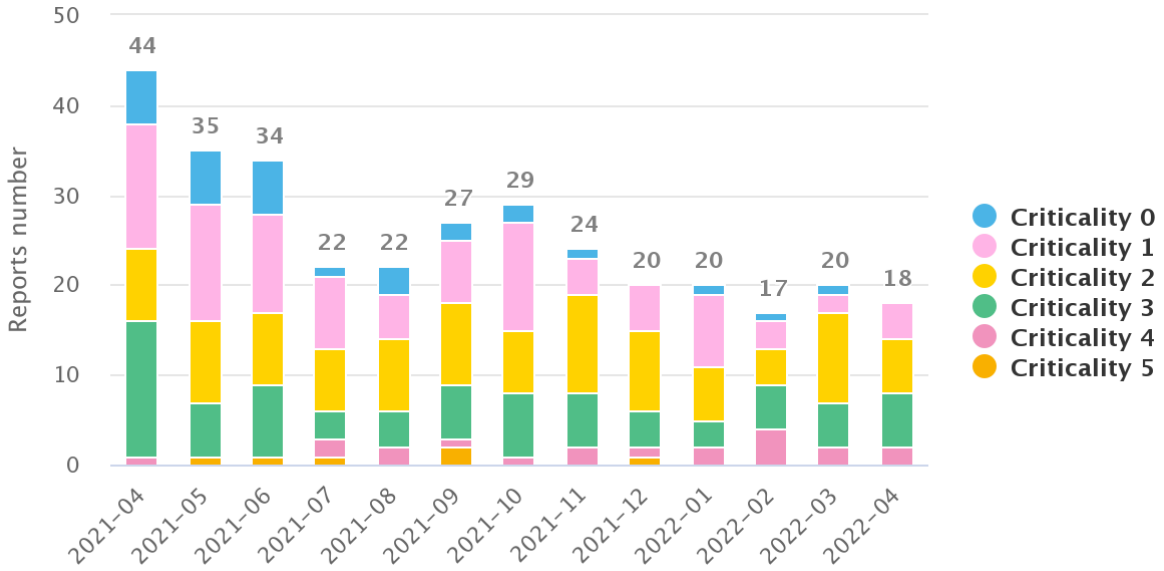
With the changes in the delivery of the Signals and World Watch services, all customers have been given complimentary access to World Watch via the customer portal. This access is available until May 31, 2022, if you are not a current subscriber and wish to continue receiving the advisories after this date then you can contact your Service Delivery Manager to sign up for World Watch.

At a glance

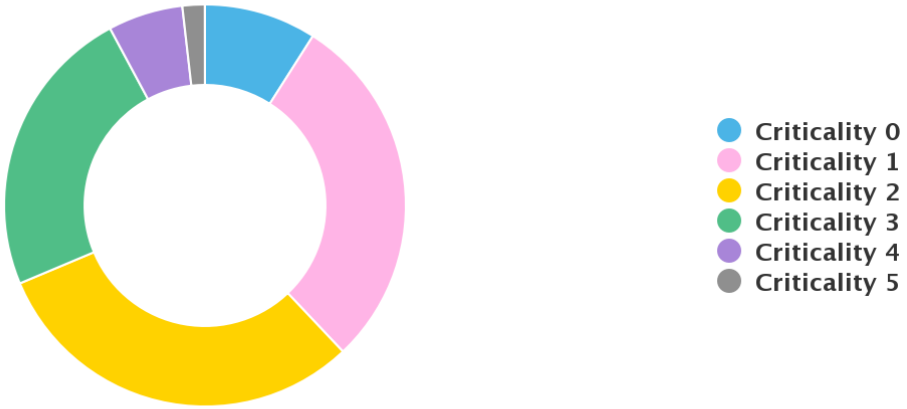
Our World Watch service is currently freely available to all customers via the customer portal until May 31, 2022. If you are not a current subscriber and wish to still receive the advisories after this date please contact your Service Delivery Manager.

World Watch Review April 2022

The Orange Cyberdefense CERT published a total of 18 new World Watch advisories during April 2022, along with adding updates to a further 17 previously published advisories. This has been a relatively quiet month when compared with the previous 12 months, however, it is in line with the numbers published so far year to date.



Breakdown of Published Advisories Previous 12 Months



Breakdown of Advisory Criticality for Previous 12 Months

VMware Critical Flaws

The most critical advisory published in April, SIG-602375, referred to a critical security advisory released by VMware addressing eight flaws in five of their products, with five of the vulnerabilities rated as critical and potentially leading to remote code execution (RCE).

When initially reported on April 7, we assigned this a criticality rating of 3 out of 5 as there were no reports of any in the wild exploitation and no proof-of-concept code was available. However, a week later we added an update to our advisory raising the criticality to 4 out of 5. This was after multiple proof-of-concept (PoC) exploits had been published publicly online for the vulnerability tracked as CVE-2022-22954 which is a remote code execution (RCE) flaw affecting VMware Workspace ONE Access and Identity Manager.

Following the release of the PoC's attempts to exploit the vulnerability in the wild had also been detected by cybersecurity intelligence organisations. At the time of the update being added we additionally reported that a Shodan search had revealed that more than 700 instances were detected that were potentially vulnerable to an attack.

Advisory Summary

The majority of the other advisories published were rated as low or medium criticality and split fairly evenly between Threats and Vulnerabilities. Some of advisories of note are:

SIG-605695 - Incorrect implementation of ECDSA in Java 15-18 validates blank signatures

- Java's flawed implementation of popular signature algorithm ECDSA allows attackers to forge valid signatures. The flaw was patched in the April 2022 Critical Patch Update which should be applied to all servers running any Java 15, 16, 17 or 18 version.

SIG-607019 - New Black Basta ransomware operation targets German, French and US-based companies

- The new ransomware gang known as Black Basta claimed responsibility for the attack on the American Dental Association (ADA) and began leaking their data on their leak site. Not too long after however the ADA disappeared from the leak site, at the time of writing though there are now 25 alleged victims listed on the Black Basta leak site.

SIG-605325 - Container escape bugs located in the AWS hotpatch for the Log4Shell vulnerability

- Unit42 researchers identified serious security issues in AWS hotfixes for the Log4Shell vulnerability and reported it responsibly to the US cloud provider. Amazon have released new versions to fix these vulnerabilities on April 19. Despite the complexity involved in exploiting these vulnerabilities users should apply the updates at the earliest opportunity.

SIG-604057 - Microsoft April Patch Tuesday fixes three serious vulnerabilities

- In their standard monthly Patch Tuesday release for April 2022, Microsoft released patches for 117 vulnerabilities, including:
    - 1 vulnerability exploited in the wild,
    - 1 with a PoC available
    - 1 considered as critical.

Editor's Notes (Beta)

This section is relatively new and was introduced in the January 2022 monthly report. Here the team will provide commentary on a news item, expansion on something specific such as a single incident, or could be as expansive as coverage on trends observed in the threat landscape.

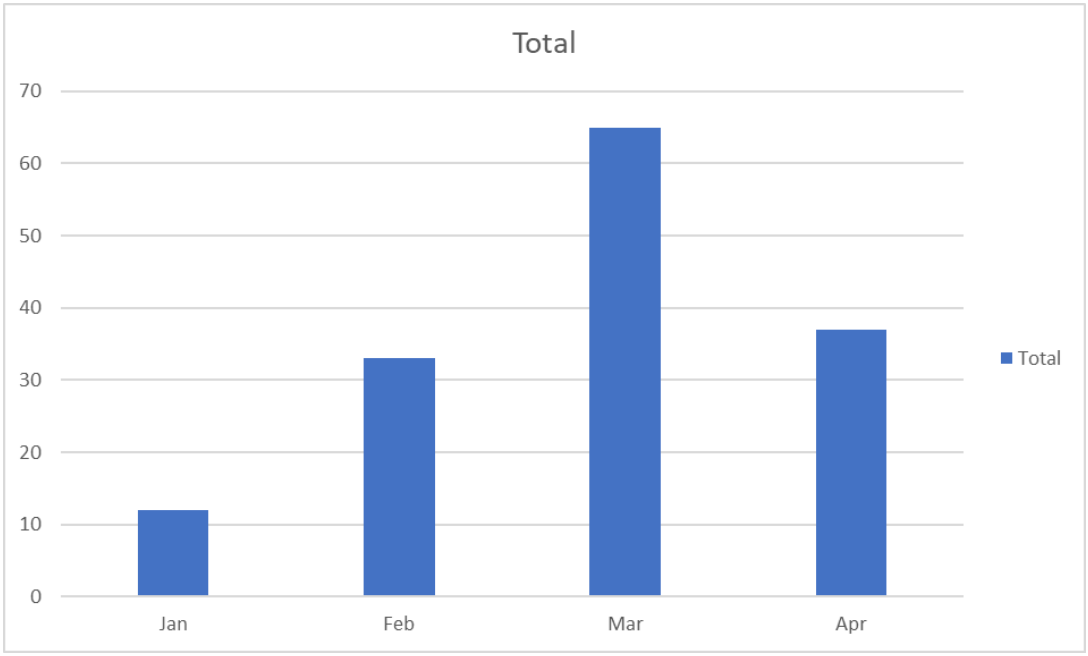
Carl

Conti Continues

It would appear that the Conti cyber-extortion (Cy-X) gang is seemingly impervious to any actions aimed at disrupting their criminal activities. Whether these actions are from Government or law enforcement agencies attempts to identify any of the individuals involved in the gang, or even from their own potential "insider threat" in the form of the "Conti Leaks" Twitter account which dumped internal data of the group including chat logs and source code, Conti seem able to maintain and even increase their operations.

Indeed, once the full extent of the so-called Conti Leaks began to be appreciated it was fully expected to force the gang to at least pause operations whilst they re-tooled and established new operational infrastructure and processes, similar in some ways to what their victims whose data is encrypted are forced to do. It was even surmised that they may end up having to cease operations entirely for a period before rebranding and returning in a different form. However, it is widely reported that the opposite of these beliefs is true, and whilst security analysts were still poring over the contents of the leaks it seems the gang was busy either building new infrastructure or bringing online already provisioned backup infrastructure which allowed them to maintain their activities. To be fair, given how business like these prolific cyber extortion gangs are known to operate, it's not a stretch of the imagination to consider that they have a robust business continuity plan in place.

In fact, as the chart below highlights, our own analysis of the leak site maintained by Conti shows that there was a sudden surge of victims published in March despite the leaks which began on February 27.



If anything, the gang seem to be going from strength to strength with them currently being considered public enemy number one by the Costa Rican government following attacks against their systems causing the country to declare a national emergency. The attacks have targeted at least five different agencies:

- the Ministry of Finance
- the Ministry of Labor and Social Security
- The Social Development and Family Allowances Fund
- the Interuniversity Headquarters of Alajuela
- JASEC, which runs the electricity in Cartago, a city of about 160,000 people

The gang have also announced that they have a 672GB data dump containing stolen information from the affected agencies of which, at the time of writing, 97% has already been published on the Conti leak site.

Despite appearances the authorities are not resting in attempting to combat the threat the Conti gang pose to businesses globally. The United States is certainly seeming to take the lead in this regard and recently offered a reward of up to $15 million for information pertaining to the Conti gang. With $10 million on offer for information that leads to the identification or location of leadership members of the gang and the other $5 million offered for information leading to the arrest and/or conviction of any individual conspiring to participate in or attempting to participate in a Conti ransomware incident. This action comes after the FBI had previously estimated that as of January 2022, there had been over 1,000 victims of attacks associated with Conti ransomware with victim pay-outs exceeding $150,000,000, although in reality this figure is likely to be conservative due to unknown victims having paid the ransom.

Whether or not these offers of financial reward will be enough to convince someone to turn against Conti remains to be seen, especially given the already high financial rewards cyber extortion currently brings. Even if high ranking members of the gang can be identified, the question then remains as to whether

anything can be done about them depending on their locale given that they are Russian speaking. Whilst there was some previous collaboration between the United States and Russia resulting in the arrest of members of the REvil group, given the current tensions between Russia and the West the likelihood of such collaboration in the near future appears slim.

Charl

Trust, interdependence, contagion and resilience

In a presentation I recently delivered in Belgium I made the argument that the concept of 'trust' should be viewed as part of the essential 'infrastructure' upon which modern societies and economies are built. I used the analogy of the complex road network that enables us to cross vast distances quickly and comfortably. This incredibly enabling facility is made possible because, as drivers, we have trust in all the elements that make up the roads and traffic system – the materials, engineering, rules, qualifications of drivers, regulations, and law enforcement. If any of these elements were to fail, or if we were to lose our trust in any of these elements, no one would be prepared to drive at speed and our societies and economies would be severely impaired.

The same is true for the digital systems that have now become (literally) essential to the smooth functioning of modern societies and economies. Not only must the multitude of complex layers of technology, people and processes all work as designed, but we must trust that they are working as required in order for societies to benefit from them. Imagine for a moment what would happen if we stopped trusting the mathematical outputs produced by core business technologies like Oracle or SAP, or even Microsoft Excel! No process or program that relied on data produced by the calculations of these systems would be considered reliable, and every transaction or decision based on these numbers would also fall into doubt. Countless services, businesses and ecosystems world-wide would ground to a halt.

Our trust in the confidentiality, integrity and availability of core technologies is therefore essential to the continued functioning of modern societies. As Dr Dan Geer puts it: "cybersecurity and the future of humanity are now conjoined"[1]

I proceed in my presentation to argue that the loss of trust is contagious. In other words, once trust is lost somewhere for someone, this loss of trust spreads rapidly across a system.

It all sounds a bit dramatic, but there's a powerful real-world example of contagion[2] in action in the 2008 Global Financial Crisis, where the risk was shared across many businesses in a way that ultimately impacted a wide range of sectors. When the housing bubble burst, it created a 'contagion effect' that brought the entire system crashing down.

[1] https://www.hoover.org/research/rubicon

[2] http://www.brainstormmag.co.za/business/14549-the-contagion-effect

In 2014 the Centre for Risk Studies at Cambridge University ran a study, in which they developed a detailed risk scenario describing a slow burning cyberattack on a fictional software developer that has global consequences. The improbable but plausible scenario is based on a variety of real (but smaller) cases.

Called the Sybil Logic Bomb Project3, the scenario describes a malicious insider who modifies the source code in a regular upgrade of the Sybil (the company is fictional) database software. The 'bomb' is designed to slowly corrupt data by introducing small errors in the systems — errors so small that they are not noticeable at first. Because Sybil software is popular software used by many companies, the bomb gets distributed into the information systems of companies around the world within a few weeks. Imperceptibly, the virus damages and undermines business systems over a period of several years.

The damage caused by the more extreme variants of Sybil Logic Bomb is almost as severe as the Great Financial Crisis of 2007-2012. The most extreme scenario variant, X1, shows a GDP at Risk of $15 trillion, in comparison to the damage of $20 trillion caused by the Great Financial Crisis of 2007-2008.

The contagious nature of risk (and the loss of trust) in cyberspace is an emergent property of 'interdependence'. As Dan Geer puts it in the paper cited above: "because the wellspring of risk is dependence, aggregate risk is a monotonically increasing function of aggregate dependence". "Because dependence is transitive, so is risk. That you may not yourself depend on something directly does not mean that you do not depend on it indirectly. We call the transitive reach of dependence 'interdependence,' which is to say, correlated risk".

At Orange Cyberdefense we've focused on this for a long time now. As we discussed in our annual 'World 2021' keynote panel, 'Interdependence' describes how IT systems and the businesses that use them do not operate in isolation. Security risk cannot be assessed or managed for a single business in isolation, and the impact of a breach or compromise is never restricted to the primary target alone. It's not just about upstream or downstream technology exposure, it's about the fundamental reality that we operate within a complex 'web' of technical and business relationships, that make the probability and impact of security failures exponentially larger than we think.

The issue of interdependence as a fundamental attribute of cyberspace suggests that supply chain attacks will continue to be a threat, and the overwhelming success of the big supply chain attacks of the past (like SolarWinds) is going to motivate even more attacks of this kind.

In a book by Timothy Geithner, Ben Bernanke and Henry Paulson on the Global Financial Crisis[4], the authors make the argument that in a complex, interdependent system that relies on trust (like finance, or cyberspace) the key to maintaining trust is to respond quickly and decisively in the face of a failure,

[3] https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-sybil-logic-bomb-cyber-catastrophe-stress-test.pdf

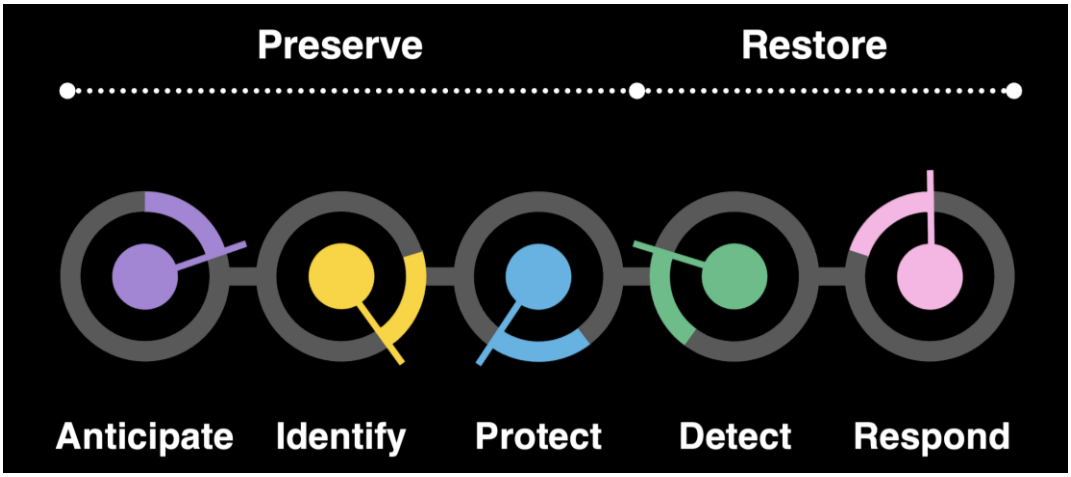
[4] https://www.amazon.co.uk/Firefighting-Financial-Crisis-its-Lessons/dp/1788163362

before it becomes a crisis. This in turn requires us to detect a failure (think compromise or breach) early so that we can respond quickly.

Geer has a different way of saying a similar thing: “Mean Time To Repair (MTTR) of zero (instant recovery) is more consistent with planning for maximal damage scenarios. The lesson under these circumstances is that the paramount security engineering design goal becomes no silent failure – not no failure but no silent failure – one cannot mitigate what one does not recognize is happening”[5].

The point of it all is this: In a complex, interdependent environment (like cyberspace), failure, however scarce we can make it, is inevitable. As John McAfee famously put it, “Any logical structure that humans can conceive will be susceptible to hacking, and the more complex the structure, the more certain that it can be hacked”[6].

When systems fail trust is lost, and the loss of trust is contagious, meaning that the compound impact of a failure across the entire system can be exponentially larger than we would otherwise predict. Per Geithner et al, the key to preserving trust is the ability to detect ‘failures’ and respond quickly and decisively.



This essential balance between preserving and restoring trust is also cleanly reflecting in the various activities of the NIST Cybersecurity Framework[7], as well as our own, adapted framework, as illustrated above.

5 https://cyberdefensereview.army.mil/Portals/6/Documents/2022_winter/17_Geer_CDR_V7N1_WINTER_2022_Special_Edition.pdf?ver=nv5jlxqLIDV3URtBPhO2mw%3d%3d

6 http://www.newsweek.com/advanced-artificial-intelligence-hacks-itself-587675

7 https://www.nist.gov/cyberframework

Wicus

Defined by Risk and Vulnerability

Google has an initiative called ‘Project Zero’ (P0) that is tasked with finding vulnerabilities in any product. These vulnerabilities are termed zero-day vulnerabilities as there are no security fixes for these. The team is also tasked with dissecting and identifying exploits that are used against targets by other attackers.

The P0 team disclosed statistics for 2021 showing that they tracked 58 security vulnerabilities that are considered zero-day and were exploited in the wild. Compare this with 2020 that only saw 25 zero-day vulnerabilities being exploited in the wild, while P0 only recorded 20 zero-day vulnerabilities being exploited in 2019.

The bulk of the zero-day vulnerabilities were attributed to Google Chrome with 14 zero-day vulnerabilities being exploited in the wild. This was followed by Windows (10), Android (7), WebKit (7), Exchange Server (5), iOS(5), Internet Explorer (4), etc. Of the top seven products, three products listed are classified as browsers (Chrome, WebKit, Internet Explorer) and two products are classified as mobile operating systems (Android, iOS). The remaining two products are from the Microsoft stable and are classified as desktop operating system (Windows) and traditional on-premise enterprise application (Exchange Server).

Bear in mind that the P0 statistics are tracking zero-day vulnerabilities exploited in the wild. This means someone found a vulnerability and crafted an exploit or chain of exploits. For the most part malicious intent is behind some of these exploit chains, but in some edge cases the vulnerabilities were found as part of an ethical research project. The latter representing a small proportion of the total body of zero-day vulnerabilities considered as “exploited in the wild”.

Maddie Stone, a team member of P0, indicated in a Wired article published in April 2022 that there exists a considerable blind spot when it comes to certain products. There is just not enough data on some of these products to detect attempted zero-day exploitation.

Is it then a good thing that we have so many zero-day vulnerabilities in a popular product such as Chrome? Ideally, we would like to have none. Realistically that is only a wish or a dream. We know that almost all software has some weaknesses. We can also assume that there is a greater than zero chance that some of those weaknesses could be used to undermine confidentiality, integrity, or availability. By that assumption we expect to observe a much larger list of vulnerable products. This reality is then compounded even further when software is combined in complex systems. The factor grows at an impressive rate, meaning that there will always be latent vulnerabilities with the potential to increase the risk exposure at the drop of a hat.

This risk acceptance and the management of that risk are the only tools available to a modern business when it comes to its cyber security. To exist as a modern business, you need to accept that vendors will supply incomplete solutions, systems, products, software, etc. with defects that can lead to some business impact.

The challenge with cybersecurity is that exploitation of these vulnerabilities can go unseen for days, weeks or even months. The scale of exploitation can also grow fast due to the use of computers to help automate the attacks.

Approaches such as ‘Zero-Trust’ can go a long way to limit the impact of vulnerabilities. The challenge is to put checks-and-balances in place that, by default contains the impact, detect anomalies, and report them.

Established professions such as civil engineering, aerospace engineering, electrical engineering, etc. are guided by well developed and tested principals, techniques, and mathematics. These professionals practicing their craft know that their decisions, calculations, and implementations have profound impact on those around them. Bridges can collapse, airplanes can crash, or people can receive a fatal electrical shock. Would it then be fair to expect the same level of completements or rigor from those building information systems?

To what standard do we hold “software engineers” accountable. What does it mean to be a software engineer or is the field of computing and software just so immature that we are at the early stages of trial and error? How many iterations do we need to endure before we realize that there is a step up required?

It is not clear what a mature “Information Technology” or “Information Security” profession looks like. Sadly, I believe we have some way to go.

Tales from the Trenches (Beta)

The cyber threat presented by Russia, Iran, or China is unlikely to subside. These countries have various reasons to further their interests and cyberspace has proven to be a very effective way to do so.

All three countries have suffered sanctions of one kind of another, with Iran arguably the one suffering the most. Russia is yet to feel the impact of the sanctions levied against if for the war it brought to Ukraine. China seems unperturbed by the sanctions levied against its telecommunications equipment and mobile phone manufacturers. The U.S. and its allies are valid cyber targets in the eyes of the governments of China, Russia, and Iran. China uses cyber operations to further its long-term strategic goals, while Russia and Iran use cyber operations to seek a more aggressive response to the West.

Espionage is a common theme when examining cyberattacks attributed to various nations. Unfortunately, this does not end there as authoritarian governments are also known to use their cyber capabilities to identify and spy on dissidents or refugees fleeing reprisal. China and Iran are believed to be guilty of this. The countries have trained agencies or groups that specialize in using cyberspace to further the goals of the countries they represent. These agencies are faceless, and cyberspace allows their activities to go almost unnoticed, implicitly cloaking those operators. Attribution is thus very difficult and almost impossible without the assistance of multiple capable government agencies. A lot of work and effort has been done in this space and western governments, with the aid of the private sector, managed to pull back the curtain that hides some of the activity in cyberspace, revealing some of the actors. Some of these groups leave clues that can be used to tie them to something that then leads to further discoveries.

Threat groups APT10 and APT41 are attributed to China. The former is strongly associated with the Chinese Ministry of State Security's Tianjin State Security Bureau. APT10 is known to target companies with ties to defense and the military industrial complex and is associated with the cyber espionage campaigns designated 'Operation Cloud Hopper'. APT41 on the other hand has been observed to target telecommunications companies, but the group has also shown to be financially motivated. APT41 has a fondness of the PlugX malware and conducts spear phishing attacks against some of their targets. APT41 is known to target any government or company, including those situated in Asia.

The group tracked as APT33 is attributed to the Iranian government and is believed to have been active since at least 2013. APT33 is known to have targeted companies across the globe gravitating toward companies that specialize in the energy sector or aviation sector. The group is known to use an extensive array of publicly available hacking tools and leverages phishing as means to obtain credentials. APT33 is mostly known for its cyberespionage activities but has been observed deploying destructive malware.

Russia is not afraid to use its cyber capabilities to disrupt, damage, or even destroy their targets. Years long aggression against Ukraine is evidence of this. APT28 and APT29 are attributed to Russia and are even described as reporting into distinct military (GRU) and intelligence (SVR) structures respectively inside the Russian government. The APT28 group is known to be responsible for the hack on the Democratic National Committee and the compromise of Hillary Clinton's emails linked to her election campaign. APT28 is also believed to have close ties with a group tracked as Sandworm from the same Russian Agency. Sandworm is responsible for the attacks against the Ukrainian power grids in 2015 and 2016, as well as the destructive malware known as NotPetya that caused billions of dollars damage in 2017. APT29 is accused of being behind the SolarWinds supply chain breach of December 2020.

This attack resulted in many clients of SolarWinds to effectively have a backdoor created inside their businesses.

The recent cyberattack against the Viasat KA-SAT satellite service that resulted in thousands of devices being unusable after a malicious software update was issued, was formally attributed to Russian agents of the GRU. This tactic of disruption or destruction is a known trait of the GRU.

Electronic Warfare (EW) equipment of the Russian military was recently captured by Ukrainian fighters. The equipment can perform jamming of satellite communications, jamming of other radio communication, as well as damaging other EW equipment. These capabilities are expected and common for military application, but it also shows how closely the tactics of APT28 and its kin, Sandworm, follows military doctrine.

Both APT28 and APT29 are proficient in brute forcing their way into an organization's infrastructure. APT29 is said to have extensive capabilities to target, compromise, and leverage cloud services. APT29 is known to be stealthy when they choose and can blend into an environment using valid accounts, services or tools.

Another tactic seen used by Russian agents is the recruitment of insiders working for companies or organizations of interest. Sweden recently reported such a case where a consultant leaked information to someone associated with Russia. This type of tactic is reminiscent of the cold war era, but it reminded us just how complicated security for companies really is. Unfortunately, it is not just covert government agents that we need to consider. Criminals specializing in cyber extortion (cy-ex) are also recruiting insiders to gain access to the soft unprotected insides of a business.

It is unlikely that any of these kinds of threats, be it governments, criminals, or activists, will disappear. This does tax defenders as they must be able to anticipate, identify, protect, detect, and respond to threats as effectively and efficiently as possible. Dealing with attackers backed by government agencies is scary and looks potentially impossible. These attackers have near infinite budget where most corporate security or IT budgets pale in comparison.

We believe that it is possible to stand your ground against these threats. Continuously improving and adapting will make it harder for attackers and it will require them to work harder.

Examples of actions that can help:

- MFA Strategy
    - MFA using SMS codes must be avoided as these are not strong enough.
    - MFA with push notifications can be bypassed if attackers with stolen credentials spam the prompt notification resulting in the victim pressing Accept/Approve to make the notification stop. A strong form of MFA is using dedicated physical devices for authentication. One such example is those supporting the FIDO2 standard such as YubiKeys.
- Identity and Access Management
    - IAM must be reviewed regularly to limit the potential for privilege escalation, abusing account recovery mechanisms, or abusing dormant accounts.

  - Removing accounts from the system needs to be automated and should follow clear procedures. For example, when staff or contractors no longer work for the business, then these accounts must be disabled immediately, followed by a deletion process. This exercise should extend to include machine or service identities as attackers will use these to blend in.
  - Anomalous or suspicious authentication attempts must be investigated and responded to. This will require a system that knows what is acceptable behavior and what needs to be flagged.
- Monitoring of all environments.
  - Activity on cloud environments must be monitored to detect anomalous activity and this could result in blind spots if not reviewed regularly.
  - Secure remote access services such as VPNs and Virtual Desktop Interface/Remote Desktop must be monitored for suspicious activity as these perimeter services are frequently targeted.
- Penetration tests or goal oriented red team activities
  - Engage regularly to test assumptions of your defenses.
  - Act on the recommendations to reduce risk.
  - Accepting risk or deferring risks is perhaps acceptable for the short-term but is a poor long-term strategy.
- Distributed Denial of Service attacks
  - Ensure critical systems are protected and that you can recover from various types of denial-of-service attacks based on how your business functions.
  - Architect systems so that DDoS attacks can be mitigated or impact lessened.
- Insider threat strategy
  - Early detection of anomalous or suspicious behavior is important, but there is a thin line to walk here. The key here is not to turn the business into a police state, but to enable staff to be productive within their line of work and at the same time limit the impact of a rogue employee or contractor.
  - Technical controls can be put in place to prohibit unauthorized actions. Continuous violation must be acted upon.
- Vulnerability Management
  - This is a continuous process.
  - Automation is important, but not all systems can be kept up to date without human assistance due to complexity, etc.
  - Have a strategy for legacy systems or systems that have significant business impact that cannot be patched easily or at all.

Good News Cyber

A third member of the infamous FIN7, also known as the 'Carbanak Group', was sentenced to five years in prison in a U.S. court. The team member specialized in gaining access to the computer systems of organizations and was 'employed as a pen tester'. The group was active from 2013 and performed in various financial fraud activities. The FIN7 team was very successful in stealing Payment Card details from US-based restaurants and retailers, with an estimated 20 million customer card records pilfered. It is believed that the group managed to breach computer networks of businesses in all 50 states of the US. The group did not limit their activities to just the US but also breached computer systems in the UK, Australia, and France.

The Binance cryptocurrency exchange had to freeze $5.8 million worth of cryptocurrency in response to attackers said to be North Korean agents. The frozen digital currency was part of a bigger heist of nearly $540 million worth of Ethereum and a cryptocurrency named USDC that is linked to the US dollar. North Korea is known for targeting cryptocurrency exchanges. This recent ship to target the Decentralized Finance (DeFi) platform named Ronin Network is a sign of more attacks to come. DeFi is a new approach being tested to create a less regulated environment free from central bank or governmental oversight using blockchain technologies to keep track of ownership and carry value. The Ethereum project defines DeFi as ".. an open and global financial system built for the internet age – an alternative to a system that's opaque, tightly controlled, and held together by decades-old infrastructure and processes." Some DeFi platforms represents value through using Non-Fungible Tokens (NFT). NFT's represents ownership over a digital asset such as digital art or in the case of Axie Infinity digital in game assets such as characters, land or items.

Microsoft recently announced that they will be making their Microsoft Defender for Business available to small and medium enterprises. The pricing will also be favorable for these businesses as Enterprise grade solutions of similar caliber is generally priced beyond what these classes of business can afford. Microsoft Defender for Business is already bundled as part of Microsoft 365 Business premium if the employee count is less than 300. SMEs can now also license Microsoft Defender for Business as a standalone solution. Defender for Business provides Enterprise level Endpoint Detection and Response (EDR) capabilities and has a wider range of capabilities compared to traditional anti-virus. Defender for Business also integrates with Microsoft 365 Lighthouse that allows Managed Service Providers (MSPs) to assist with administration and triage of customer sites. Microsoft also bundled support for Remote Monitoring and Management (RMM) tools in Defender for Business to further improve serviceability for MSPs.