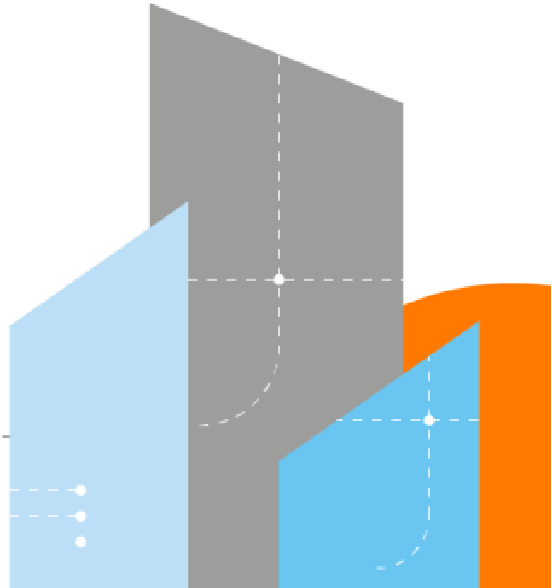
Orange
Cyberdefense

Security Intelligence

Monthly Report

August 2022



CONTENTS

INTRODUCTION

August 2022 saw many smaller countries announcing that they fell victim to cyberattacks. These countries blame larger geopolitical entities for their woes.

Taiwan claimed that its government websites were targeted by attacks it attributed to China. This incident coincided with U.S. House Speaker Nancy Pelosi's visit to Taiwan. Diplomatic tensions between Albania and Iran reached new levels when it was revealed that that the cyber division of Iran's Revolutionary Guard Corps (IRGC) targeted Albania's government with wiper ware. Albania later moved to cut diplomatic ties with Iran. Montenegro also announced that it was being targeted by what it believes to be hackers with ties to the Russian government.

Threat actors associated with the Iranian government were in the news, with Mandiant citing a new group it tracks as APT42. APT42 might be an umbrella cluster of the IRGC. Mandiant released another report covering an espionage operation by another Iranian group tracked as UNC3890. This group was observed targeting Israeli healthcare, shipping, government, and energy sectors.

Microsoft published a report on a subgroup of the Phosphorous group. Phosphorous is also linked to the Iranian government, but Microsoft believes the new subgroup tracked as DEV-0270 is conducting ransomware operations for personal gain.

Microsoft shared details on malware linked to Nobelium, also known as APT29 or Cozy Bear. The malware called MagicWeb allows for a persistent backdoor into a compromised Active Directory Federated Service (ADFS) host. The infected ADFS also allows an attacker to authenticate as anyone and bypass any MFA interaction.

The highly active and infamous cyber extortion group LockBit 3.0 has recently introduced new features to its Ransomware-as-a-Service capabilities. It now allows negotiation chat logs with victims to be easily accessible if it so chooses. Also, LockBit expanded the number of supported payment options by introducing support for Zcash in addition to Monero and Bitcoin.

LockBit also claimed that its infrastructure was hit with a distributed denial of service (DDoS) attack. It claims that this was retaliation by Entrust, a victim that LockBit claimed in August 2022.

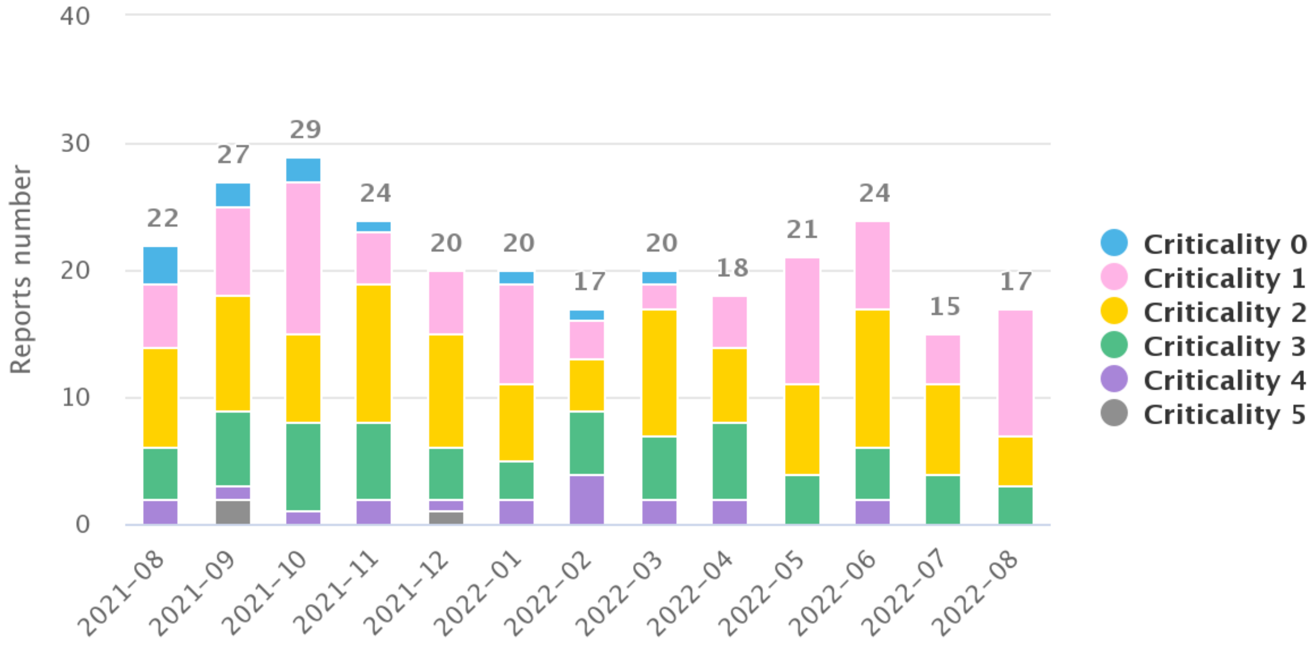
LastPass, the password management firm, announced that it suffered a breach that saw attackers stealing proprietary information relating to its software offerings. LastPass did indicate no sensitive customer data or passwords were leaked.

At a glance

LockBit 3.0 claims that its infrastructure was experiencing a distributed denial of service (DDoS) attack that it attribute to retaliation of Entrust, which LockBit 3.0 claimed as a ransom victim.

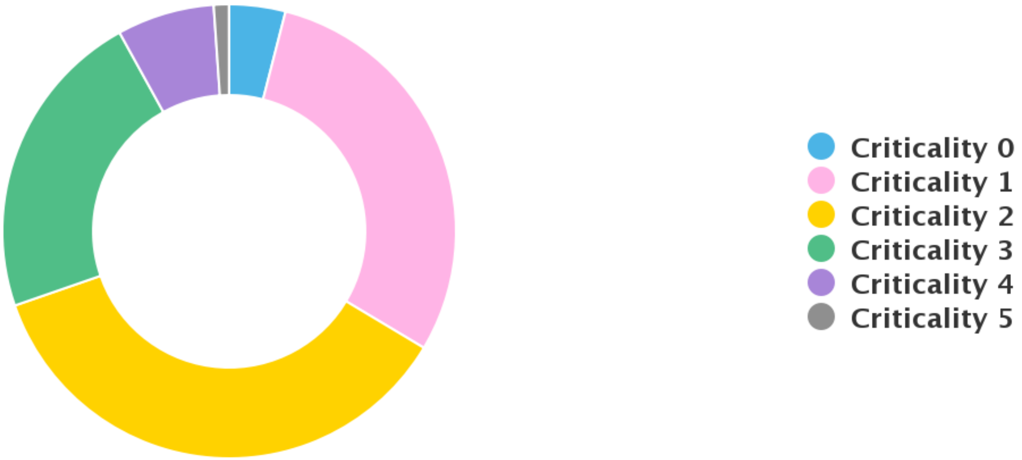
World Watch Review August 2022

The Orange Cyberdefense CERT published a total of 17 new World Watch advisories during August 2022, along with adding updates to a further 26 advisories. This volume of new advisories is a slight increase on last month's figure; however, the large number of updates published to advisories serves to highlight the work our CERT put in to stay abreast of any new developments as they arise and then communicate any relevant details to customers, including any changes in criticality or guidance.



Breakdown of Published Advisories Previous 12 Months

The criticality levels allocated to the August advisories again remained low. The highest allocated criticality was level 3, with only three of these being published this month.



Breakdown of Advisory Criticality for Previous 12 Months

Advisory Summary

As can be seen above the advisories this month were all given criticality ratings of Informational (1), Low (2) or Medium (3) when initially published. These ratings are based on our CERT's assessment of the risk and threat levels associated with the subject of the advisory at the time of publication, so even though an advisory may concern a vulnerability rated as critical by the vendor we may deem it to only initially be medium, if say there is no publicly available exploit. This is under constant monitoring however and subsequent updates will increase our criticality level as required if circumstances should change. Some advisories of note this month are:

SIG-638929 - Malicious actors abuse pre-authentication RCE vulnerability chain on Zimbra email servers

- On August 10, Volexity researchers published a report in which they announce that Zimbra Collaboration Suite mail servers are vulnerable to a chain of vulnerabilities that allows an attacker to carry out a remote pre-authentication code execution. This chain includes CVE-2022-37042 and CVE-2022-27925. CVE-2022-37042 is a vulnerability that allows an attacker to bypass valid administrator authentication. Using this, attackers can gain access to prior authenticated administrative sessions that are required to exploit the CVE-2022-27925 RCE vulnerability.

- Unfortunately, Volexity reports that they have observed several attacks using this string on various organizations that use Zimbra Collaboration Suite messaging. According to their investigation, 1,000 ZCS instances worldwide have been hacked and compromised. These instances belong to various global organizations, including government departments and ministries; military branches; global companies with billions of dollars in revenue.

SIG-638037 - Recent APT31 campaign targets Russian companies

- Researchers from Positive Technologies recently unveiled a campaign from APT31 targeting Russian media and energy companies with the YaRAT malware. The campaign started with a maldoc used to extract a malicious payload packed with VMProtect. The techniques and tools were found to be identical to the ones attributed to APT31 by Positive Technologies in an earlier campaign back in August 2021. Other Chinese threat actor groups have been targeting Russian companies since at least 2020.

- APT31, also known as Zirconium or Judgement Panda, is a Chinese actor specialized on cyber espionage and data theft, focusing on obtaining information that can provide the Chinese government and state enterprises with political, economic and military advantages. The group has been active since at least 2014, when it gained access to NSA Equation Group's exploit code and repurposed it for their own use. In 2021, the French cybersecurity agency ANSSI issued an alert about APT31 compromising home routers in order to perform stealth reconnaissance as well as attacks.

SIG-642067 - The Sliver tool is increasingly used by threat actors for post-exploitation

- A recent report from Microsoft highlights how the cross-platform open-source adversary/red team emulation tool Sliver has recently been exploited by threat actors such as UNC1878 (also known as fin12), a financially motivated threat actor that monetizes network access via the deployment of the RYUK ransomware. It is also used by state-sponsored actors in Russia, most notably APT29 (aka Cozy Bear, The Dukes, Grizzly Steppe).

- Sliver has managed to stay in the shadows and remain lesser known than its famous competitor, Cobalt Strike. Sliver is an interesting alternative for players looking for a lesser-known set of tools with fewer security measures associated with it. Nevertheless, it was first made public at the end of 2019. Detections measures can be put in place to protect against it...

SIG-638483 - Microsoft fixes an elevation of privilege vulnerability exploited in the wild

- New security updates have been released by Microsoft to fix 121 vulnerabilities, including 17 classified as critical and 104 important.

- Among these vulnerabilities, of particular concern is CVE-2022-34713, which is currently exploited in the wild. Dubbed DogWalk, this is a directory traversal bug present in the Microsoft Support Diagnostic Tool (MSDT). If exploited, a remote attacker can trick his victim into executing a specially crafted "diagcab" archive file in order to execute arbitrary code. CVE-2022-34713 received a maximum overall CVSS score of 8.1 (out of 10) from our Vulnerability Intelligence Watch team.

- Microsoft has not disclosed any technical information or information about potential attacks. However, a technical writeup of the vulnerability and PoC exploit is available online since January 2020, after Microsoft had replied to security researcher Imre Rad's report it won't provide a fix since this isn't a security issue. The vulnerability has recently resurfaced in June after Follina brought attention to MSDT. It was corrected by 0patch in June, and finally by Microsoft in August.

Editor's Notes

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

IBM Cost of a Data Breach Report 2022 Summary

https://www.ibm.com/security/data-breach

The "Cost of a Data Breach Report", published by IBM & Ponemon Institute, is now in its 17th year. This year 550 real world breaches were analysed with data gathered from 17 countries and 17 industries. Whilst, as expected, much of the report does not make for pleasant reading and depicts quite a bleak view of the threat landscape, there are indications that new technologies and approaches may at least be able to help organisations reduce the costs associated with a data breach.

Average Cost

The main headline from the report is that the average cost of a data breach has now reached $4.35 million USD in 2022, the highest it's been since the report began and an increase of 2.6% on the previous year.

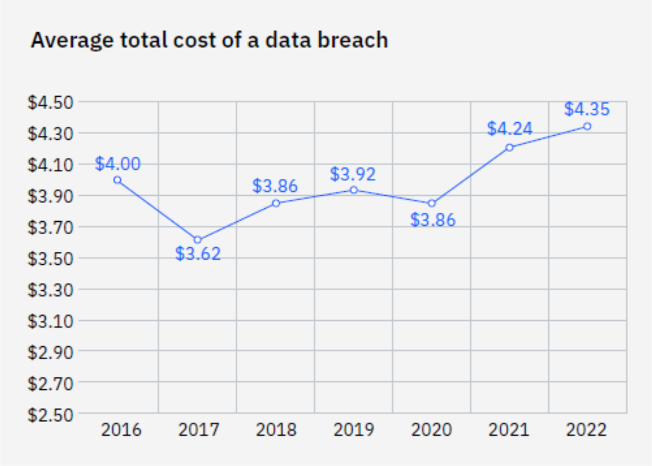


Figure 1: Measured in USD millions

The report also found that if the breach impacted a critical infrastructure organisation, then that average cost rose to $4.82 million USD. Critical infrastructure organizations included those in the financial services, industrial, technology, energy, transportation, communication, healthcare, education, and public sector industries.

For the 12th year running though the healthcare industry has the highest average cost of a breach, this has now reached $10.10 million USD which is a 41.6% increase on the value in the report published in 2020 and an increase of 9.4% from 2021.

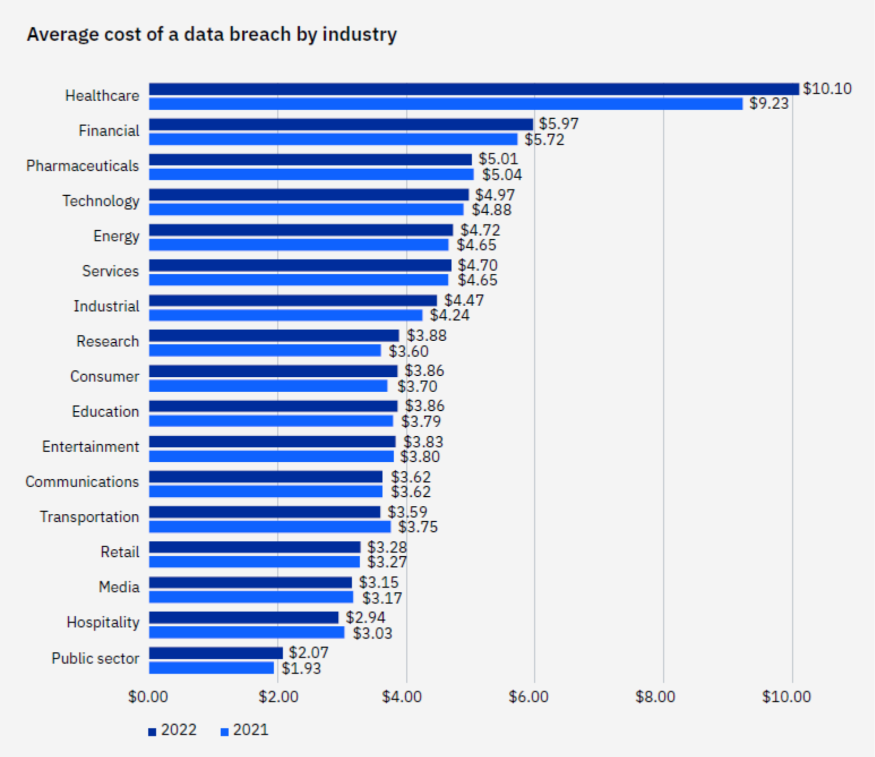


Figure 4: Measured in USD millions

When it comes to geography, again for the 12th year in a row, the United States is reported as being the costliest country or region to experience a data breach with the average total cost coming in at $9.44 million USD, an increase of 4.3% on last year's report. The country with the largest relative growth on last year was Brazil which saw a 27.8% increase from $1.08 million USD to $1.38 million USD.

The report also found that 83% of the organisations included in the study had experienced more than one data breach, which based on the figures already discussed becomes a costly affair. With this in mind though it seems that organisations are not prepared to simply absorb the cost of a data breach. Indeed, the report shows that 60% of the organisations admitted to increasing consumer prices purely to compensate for a data breach separate from other increases, for example due to inflation. If, or when, this becomes common knowledge organisations should expect to see some fallout from consumers not happy with the fact that their data was stolen, and the potential disruption that causes, and then having to pay extra for their goods and services because of it.

Mitigations

Whilst the costs associated with a data breach can be eye watering, the report isn't all doom and gloom, there are several factors that can help lower the cost of a breach. Of these factors three in particular have the most impact, the use of security platforms that use AI, the formation and use of an incident response (IR) team and adopting a DevSecOps approach all led to significant reductions in the average cost of a breach.

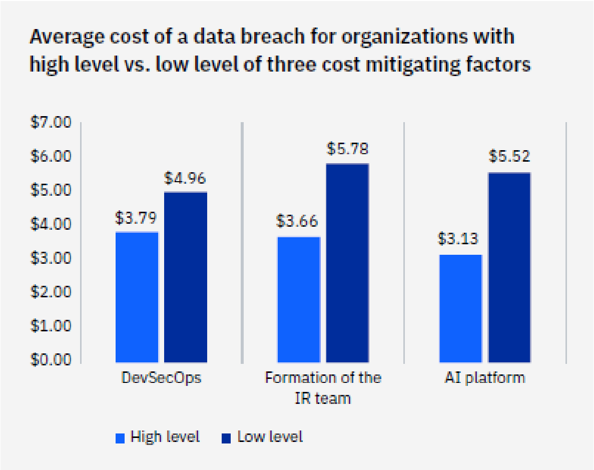


Figure 15: Measured in USD millions

The implementation of security AI and automation technologies also carried significant cost savings when compared to organisations that hadn't deployed these solutions. For the context of the report these are technologies that are used to "augment or replace human intervention in the identification and containment of incidents and intrusion attempts. Such technologies depend upon AI, machine learning, analytics and automated security orchestration."

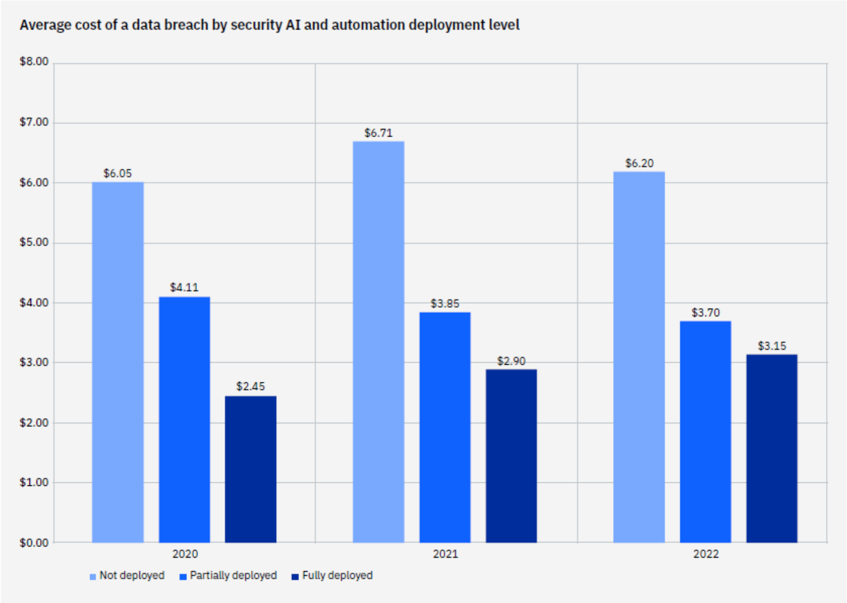


Figure 17: Measured in USD millions

Aside from the monetary savings these technologies also helped to reduce the average time taken to identify and contain a data breach. With fully deployed security AI and automation the total number of days was 249, 181 to identify and 68 to contain, whereas with no security AI and automation that increased to a total of 323 days, 235 to identify and 88 to contain.

In a similar vein, organisations with extended detection and response (XDR) solutions deployed in their environment were able to identify and contain a breach 29 days faster than organisations without XDR. The use of XDR, likely as a direct result of these time savings, was also associated with a lower-than-average cost of a data breach. With no XDR deployed the average cost of a breach was $4.55

million USD, whereas organisations with XDR reported an average cost of $4.15 million USD, a 9.2% difference.

Cloud

The recent pandemic obviously accelerated most organisations digital transformation plans, especially the adoption of and move to cloud technologies. Despite this though the report shows that 43% of organisations were only in the early stages or had not even started applying appropriate security practices to ensure their cloud environments were safe and secure. This is all the more concerning when you factor in another finding from the report showing that 45% of the breaches reported on happened in the cloud.

For the organizations that do have mature cloud security procedures the cost of a breach was $0.66 million USD less than for those still in the early stages of securing their cloud environments. Organisations with the highest maturity level reported a cost of $3.87 million USD, while the lowest maturity level in cloud security practices where no controls are used had a higher cost of $4.59 million USD.

Those organisations with the highest cloud security maturity level also benefitted from being able to identify and contain the data breach far quicker than those in the early stage or who had not even started. Mature organisations reported it took an average of 176 days to identify and 61 more days to contain a breach, 237 days in total. This is 64 days less than organisations in the early stages and more than 100 days less than organisations who were yet to start.

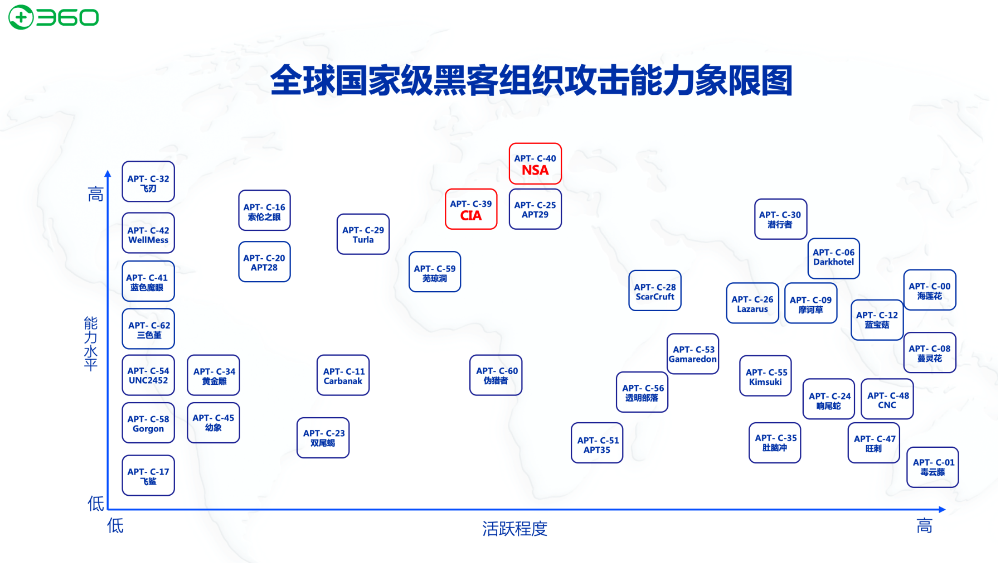
The type of cloud model used by an organisation also played a part in the severity of a breach both in terms of cost and the time taken to identify and contain the breach. A breach in a public cloud environment cost an average $5.02 million USD, and breaches within a private cloud cost an average $4.24 million USD. However, where the breach occurred in a hybrid cloud model, the cost was an average of $3.80 million USD, 27.7% less than for the public cloud. The same pattern can also be seen for identifying and containing a breach, a hybrid cloud environment resulted in a total average time of 262 days whereas in a public cloud this increased to 310 days, 16.8% longer than for the hybrid environment.

Charl

Signals in the dark

Later in this report my colleague Wicus comments on some cyber activities by western governments, and Joshua refers to the Pegasus malware, which is of course developed by an Israeli company and used by governments all around the world, in his piece below. Cyberattacks will be found in the arsenal of political tools of governments all around the world, yet in the past weeks we’ve seen some interesting efforts to shape (or reshape) public perception of who’s doing what in the cyber political space.

The first incident involves an apparent effort by the Chinese government to remind us that the west (and in particular the USA) is actively performing cyberattacks. The Chinese affair probably started when Chinese cybersecurity firm Qihoo 360 revealed the diagram below, illustrating that the US National Security Agency is the most capable of all government cyber capabilities:



http://news.sohu.com/a/583469076_362042

The NSA is described as ‘highest skill, mid level activity’.

As this Washington Post article describes, recent Chinese ‘revelations’ about NSA hacking seem oddly naive, and it’s unclear what the Chinese might be hoping to achieve by them.

However, the Chinese are probably generally-speaking correct about the US’ capabilities and levels of activity, and it serves us to remember that. While much of the ‘narrative’ in the west is understandably about the threat from so-called ‘rogue’ states like Russia, China and North Korea, we should remember that hundreds of nations develop and use offensive cyber capabilities and that cyber espionage, misinformation and other forms of cyber-attack are ‘business as usual’ for many nations, and specifically the US and her allies.

In summary: The ‘revelations’ by the Chinese about US government capabilities and activities are largely meaningless in substance but do serve as a reminder that the countries we all live in are all probably engaged in these activities. This reality does have implications for us that are maybe not immediately apparent. We will return to these later.

Another interesting development in the cyber-political landscape was a series of very forceful diplomatic actions by the nation of Albania in response to alleged cyberattacks by Iranian state-backed actors. As this article describes, “Albania severed diplomatic relations with Iran … and kicked out its diplomats after a cyberattack in July it blamed on the Islamic Republic, a move Washington supported as it vowed to take action in response to the attack on its NATO ally. Albania ordered Iranian diplomats and embassy staff to leave within 24 hours”.

This new attack has targeted the Total Information Management System (TIMS), an IT platform from Albania's Ministry of Interior used to keep track of people entering and leaving the country. As a result of this attack, six border crossing points were experiencing stoppages and delays for at least two days till the TIMS platform could be restored, according to Albania's Minister of the Interior, Bledi Chuchi. US authorities have also confirmed the attack and the attribution to Iran, adding that they were helping Albania to recover from this latest attack.

The US Whitehouse added that “The United States will take further action to hold Iran accountable for actions that threaten the security of a U.S. ally and set a troubling precedent for cyberspace". The UK government similarly renounced the Iranian attacks.

Relations between Iran and Albania have been shaky for several years now, at least since Albania aligned with the Soviets against Iran in the Iran–Iraq War in 1979, and have ebbed and flowed through several ‘seasons’ since then. More recently, in 2018, Albania accused Iran of plotting terrorist attacks in the country during the 2018 FIFA World Cup qualification, and expelled Iranian diplomats in response, including the Iranian ambassador. On the flip side, in January 2020, following the death of Iranian general Qasem Soleimani, Iranian Supreme Leader Ali Khamenei and Iranian President Hassan Rouhani made speeches smearing ‘a small and sinister country’ for trying to overthrow the Islamic regime in Iran.

This Wikipedia page provides a good summary of the political history.

On September 9, Iran's Mission to the EU accused NATO and its members of hypocrisy because they remained silent when Iran was victim of cyberattacks against its infrastructure and nuclear facilities. Iran has also accused NATO of harboring terrorists, referring to Albania hosting members of the MEK political group, an Iranian opposition party, which is highly likely the reason why Iran has targeted Albania.

What is clear is that the diplomatic response by Albania in response to the attacks, and the subsequent statements of support from her NATO allies, is highly unusual.

In 2016 the US government expelled 35 Russian diplomats as punishment for alleged interference into the US presidential elections, but such heavy-handed and public diplomatic responses to cyber-attack activity really is quite unusual, and those attacks really were unprecedented in scope and scale.

Cyber espionage, misinformation, disinformation and other ‘low visibility’ cyber-attacks that fall below a generally agreed ‘threshold’ of aggressiveness are happening all the time and are generally considered to be the ‘norm’. Where attacks are considered to exceed this ‘threshold’, the victim’s dissatisfaction is generally expressed via private diplomatic channels, and not via public pronouncements.

As a rule, when governments engage in public diplomacy regarding cyber-attacks, we consider it to be a form of ‘signaling’ – a means of sending messages or warnings via the public or to the public. The real diplomacy then happens behind closed doors, with the public signaling used as a lever to influence outcomes.

So why then this extraordinary diplomatic response by Albania? We don’t know, but several hypotheses present themselves:

1. **There are no other diplomatic channels**. One obvious explanation for this deployment of public channels for diplomacy might be that all other channels have simply collapsed. This seems unlikely, however.
2. **The attack was extraordinary**. Albanian officials allege that the Iranians "threatened to paralyse public services, erase digital systems and hack into state records, steal government intranet electronic communication and stir chaos and insecurity in the country". Much of this strikes us as 'business as usual', but the destructive outcomes described would certainly exceed the norms of cyber activity generally agreed between nations. This might be a legitimate rational for the severity of the diplomatic response. Of course, there may also be other activities (cyber or other) that the general public is not aware of.
3. **The experience was extraordinary**: Another possible explanation for the severity of the Albanian response might simply be that their experience of the incident was unprecedented by them. While the Ukrainians, for example, have weathered these kinds of attacks for several years now, countries like Greenland, Costa Rica and potentially Albania have had to endure large-scale, high-impact attacks for the first time in recent months. This would be an unusual and unpleasant experience for them, and with the correct context might result in a level of response that other, more hardened nations, wouldn't deem necessary,

Of course, these are only speculations, and we cannot know the full details of what else is happening behind the various veils of government secrecy.

Whatever the reasons for these two curious, public acts of diplomacy by Albania and China, they serve to remind us that governments all over the world (including almost certainly your own) are investing heavily in offensive cyber capabilities and activities.

Unlike almost any other domain of intelligence, military and diplomacy, cyber activities take place in a space that is also populated by civilians and civilian systems, data and even people are regularly collateral damage in these activities. The Wannacry and notPetya attack (involving Russia and North Korean actors and US capabilities) are the most obvious case in point, but there are several others, and the principle is universal.

Not only is the civilian ecosystem impacted directly by these attacks, but investments by government agencies world-wide, including in western countries, have the generalized effect of 'inflating' the security problem by developing tools, training people, spawning business ecosystems and setting precedents that inevitably 'leak' across into the civilian sphere.

Well-considered government investment into security skills and technology, intelligence and law enforcement are essential in our battle to combat cybercrime and build a safe digital world. But reckless acts and investments have exactly the opposite effect. As business and security leaders it is our responsibility to hold our governments accountable to making balanced and responsible investments in cyber that further our goals.

Wicus

Spy vs Spy

We often hear about cyberattacks launched by the East targeting businesses and governments in the West. Similarly Western news channels were eager to cover the manipulation of the US elections in 2016 using social media. It is not often that Western news publish stories where the roles are reversed.

Graphika and the Stanford Internet Observatory Cyber Policy Center published a report in which they detailed a pro-Western covert operation that aimed to generate favorable opinions about the United States. Several campaigns were uncovered stretching over five years with fake personas used to target citizens of China, Iran, but mostly Russia. The timeframe for this investigation stretched from March 2012 to August 2022.

Social media channels were analyzed, and several overlapping accounts were identified. Twitter, Facebook, and Instagram are three prominent platforms mentioned with five other social media platforms also featuring in the report. Twitter and Facebook responded by removing several accounts identified by this report.

The report claims that these campaigns, linked to an alleged covert U.S. government campaign known as the Trans-Regional Web Initiative, seems not to have “generated much genuine traction”. It is thus hard to gauge success of the impact of these campaigns by just looking at metrics linked to social media interactions. The response to posts, retweets or reshares of posts, or number of followers of the identified influence accounts. The timing of this report also falls at a time where Twitter is under heavy critique for pushing inflated user numbers and that the real user number is much lower than that claimed.

A few weeks after the Graphika and Stanford report was released, a Vice article was published that covered a story wherein the Chinese authorities publicly called out the U.S. government and NSA for attempting to “hack” a Chinese university. The university is said to be known for developing aerospace technology for military applications. The attackers attempted to phish academics of the university by sending emails with invites to conferences or events. It is not clear if these phishing attempts were successful. This does sound like the shoe is now on the other foot, as these kinds of tactics and techniques have been reportedly used by spies linked to the Chinese government. Stories like these should remind us that we live in a very complex world when it comes to government espionage and intelligence operations.

There is a saying amongst security professionals that goes something like “There is no point in planning to defend against a government backed cyberattack”. The thinking or belief is that you are most likely not going to be the target, but if you are you do not stand a chance because government backed attackers have access to resources beyond your imagination. This could be disheartening or even feel futile.

The reality is that our businesses are complex and have challenges in just defending against criminals or malicious insiders, which is most likely going to be what keep security professionals awake at night. Building secure systems requires a solid foundation including identity and access management with phishing resistant authentication, least privilege, and segmentation. This will be effective against most attacks and make it difficult for sophisticated attackers. We do not need 100% protection; we just need good detection and response to contain a breach.

Joshua

Is Pegasus the Coronavirus of tech?

Apple has always advertised their devices as being more secure than their competition and with their new lockdown mode this is no different. This has been designed in response to the growing threat of state sponsored spyware such as Pegasus. This capability is designed for the minority not the majority as high-risk people are targeted, such as journalists and politicians.

The philosophy behind lockdown mode is to reduce the possible attack surface of the device. Lockdown mode does the following: blocks most attachment types in messages and disables the link preview, stops JIT JavaScript compilation unless the site is whitelisted, stops people contacting you if you have not initiated the contact first, wired connections to the computer are blocked when iPhone is locked and finally, MDM and profiles cannot be installed once lockdown mode is activated.

To highlight how this would stop Spyware, the NSO zero-click iMessage exploit can be explored. This exploit utilises how gifs are handled in iMessages, although the .gif extension is needed for this to work. When it comes to processing the file, ImageIO is used to guess the correct format. This allowed NSO to take advantage of a PDF vulnerability. The exploit used was of a severe nature as the victim did not have to do anything to be infected. In contrast, if Lockdown mode was enabled this exploit would not have worked.

To enable Lockdown mode, the user needs to open Privacy and Security in their settings and press Lockdown mode and then press turn on Lockdown mode: this will reboot the device in Lockdown mode. In addition to this mode, Apple have made a new bounty program for findings that lead to a bypass in lockdown mode. The maximum figure paid out for this is $2,000,000 which is the highest in the industry. They have also pledged to grant $10,000,000 and any damages award in their lawsuit against the NSO Group to help organizations that fight against targeted spyware.

Although this feature has not been out for a long time and is still in its beta stages, people have already found subtle ways to bypass the USB connection. If the phone is connected to a computer and is trusted before it is put into lockdown mode, when it is put into lockdown mode this connection is still there and is not blocked even when the phone has not been unlocked. The Apple magic keyboard will still work when plugged into a phone in lockdown mode even when locked. These two examples go against Apples statement that all USB connections are blocked when the device is locked.

Overall, this is a monumental shift in the philosophy of their business, they stand to make no money from Lockdown mode and shows consumers they are at the centre for privacy and security.

Good News Cyber

Over the last couple of months, we have highlighted the efforts of law enforcement in response to cybercrime. As with any crime, it takes time to investigate a crime and then execute arrests etc. In recent years law enforcement has been much more able to act than a decade ago. More crime is committed involving technology, and this means that law enforcement must develop skills to be able to investigate potential crimes of this nature. This month we have more examples of law enforcement being able to respond to cybercrime.

The U.S. Treasury's Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash due to its alleged involvement in laundering of stolen cryptocurrency. The documents published by OFAC states that $455 million in cryptocurrency, related to a company called Axie Infinity that creates digital assets for gamification, were stolen by attackers affiliated with North Korea. Tornado Cash allegedly aided in the laundering of the stolen digital assets.

The developer of Tornado Cash, a cryptocurrency mixer or tumbler service, was arrested in Amsterdam. A mixer or tumbler service helps to obfuscate the flow of cryptocurrency from one wallet to another making it nonobvious to track. Although Ethereum or Bitcoin provides a type of anonymity, it does not do much for transactional privacy as all transactions for any given wallet are public knowledge. The developer of the Tornado Cash service was arrested within days of the OFAC sanctions announcement.

A man allegedly involved with the Ryuk ransomware team was extradited from the Netherlands to the United States. The suspect will be tried for crimes involving money laundering using cryptocurrency.

A man was arrested in connection with his alleged role in defrauding several businesses using a business email compromise (BEC) scheme. The fraud involved the fictional construction company that targeted various institution such as academia. At least two universities were defrauded of approximately $2 million. This arrest follows the extradition of three suspects from the UK also related to BEC schemes.

The U.S. State Department announced that it is willing to pay $10 million reward for information that leads to the arrest and prosecution of five individuals allegedly linked to the Conti cyber extortion group. The five suspects go by their handles of “Tramp”, “Dandis”, “Professor”, “Reshaev”, and “Target”. The Conti group has reduced their activity and is now believed to be defunct.

The Lockbit cyber extortion group recently announced that their infrastructure was the target of a distributed denial of service (DDoS) attack. Lockbit accuses Entrust of doing the dirty deed. Entrusts, a digital identity and trust management authority, recently suffered a cyberattack and Lockbit claimed that it was responsible for the incident.

Meta, the parent company of Facebook, announced that it will introduce end-to-end encryption in the Facebook Messenger application. This feature, currently only available on Meta's WhatsApp application, will improve the confidentiality of messages exchanged between parties. This decision is allegedly due to law enforcement agencies in the US forcing Facebook to hand over messages exchanged between a mother and a daughter relating to potential violation abortion laws.

The Linux Foundation with backing from the Google Open Source Security Team (GOSST) launched a bug bounty program to reward ethical disclosure of vulnerabilities in open source software. The goal of the project, called SOS Rewards, seeks to “reward a very broad range of improvements that proactively harden critical open-source projects and supporting infrastructure against application and supply chain attacks”. For more information see https://sos.dev.