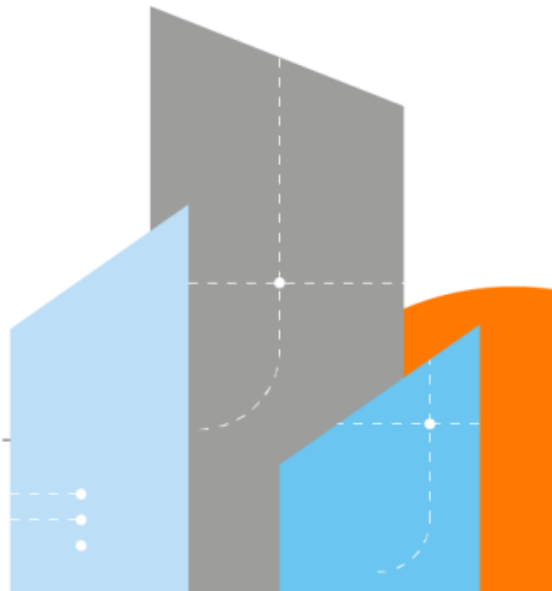
Orange
Cyberdefense

Security Intelligence

Monthly Report

October 2022



CONTENTS

CONTENTS 2

INTRODUCTION 3

World Watch Review October 2022 4

Editor's Notes 7

Chaos in the Twitter-verse 7

Victims of opportunity 8

Good News Cyber 10

INTRODUCTION

Following several weeks of blood, sweat and tears the Orange Cyberdefense Security Navigator 2023 report is almost ready.

This year's free, 126-page report includes:

- 25 pages of CyberSOC statistics
- Ransomware observations from Dark Net surveillance
- World Watch observations
- Pentesting and CSIRT stories
- Analysis of Vulnerability Scanning and Pentesting reports for the past years
- Security deep-dives into Mobile security, Manufacturing and advisory on the Ukraine war
- Security predictions: addressing four key areas of security in a different way

The report will be published on December 1st, 2022, and can be preordered here:

https://www.orangecyberdefense.com/global/security-navigator

In other news, Clare O'Neil, the Minister for Home Affairs of Australia, says the government is setting up "a permanent standing operation" that will "scour the world" and "hunt down the criminal syndicates and gangs who are targeting Australia in cyber-attacks and disrupt their efforts." It will be interesting to see how successful this "hack the hackers" initiative will be…

The US government recently released a statement concerning the International Counter Ransomware Initiative, stating that:

"The White House brought together 36 countries, and the EU, for the Second International Counter Ransomware Initiative (CRI) Summit October 31-November 1, 2022. Throughout the Summit, CRI and private sector partners discussed and developed concrete, cooperative actions to counter the spread and impact of ransomware around the globe. Over the past year, the CRI has worked to increase the resilience of all CRI partners, disrupt cyber criminals, counter illicit finance, build private sector partnerships, and cooperate globally to address this challenge."

Concrete outcomes from the summit include a commitment to enforce domestic ransomware laws, take steps to stop ransomware actors from being able to use the cryptocurrency ecosystem, lawfully disrupt ransomware actors, and to actively share information.

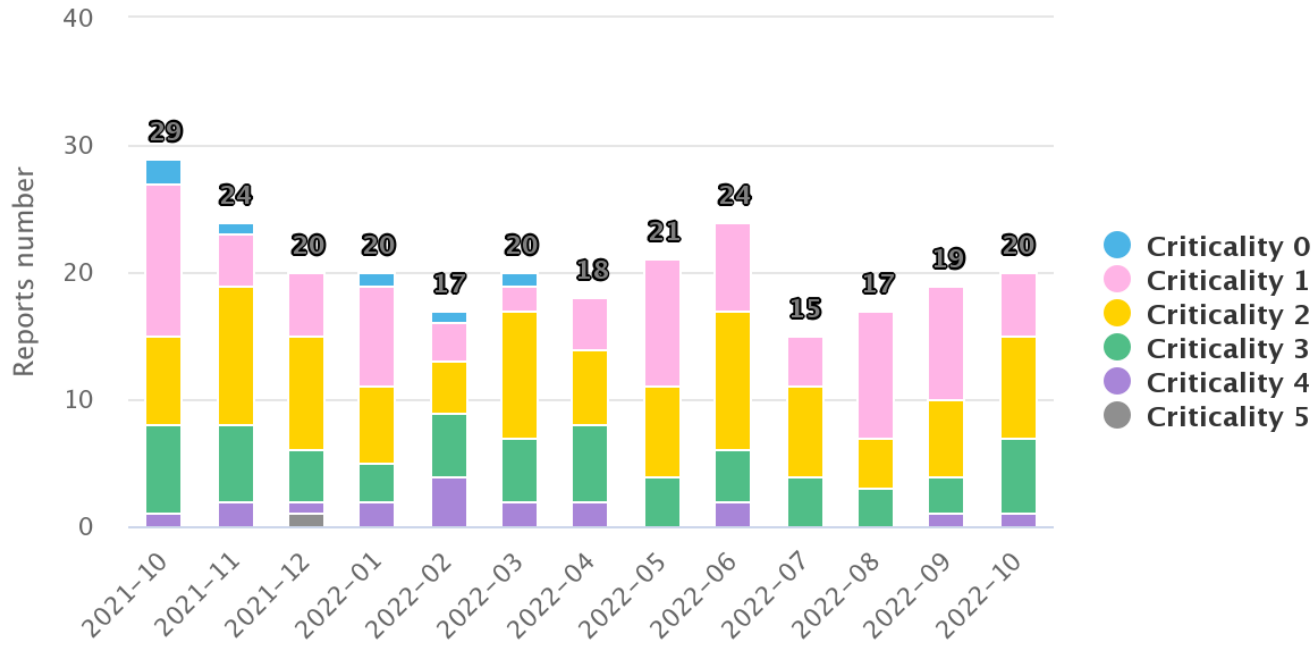
At a glance

This year's Security Navigator report will be published on December 1st, 2022.

You can get it a day early by preordering it using the posted link on this page.

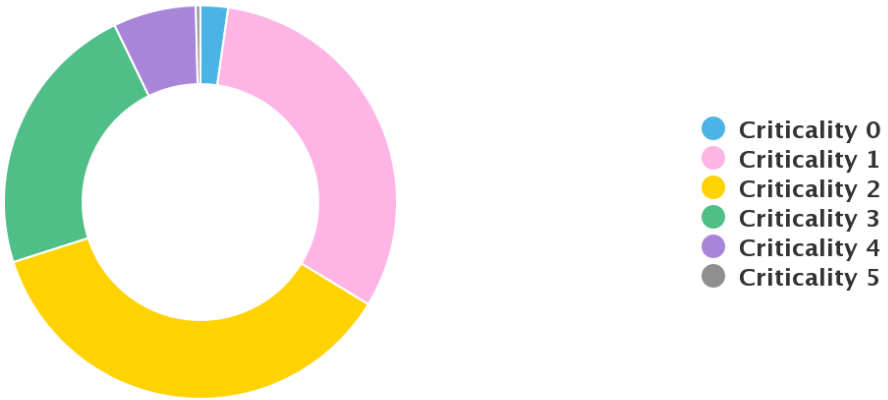
World Watch Review October 2022

The Orange Cyberdefense CERT published a total of 20 new World Watch advisories during October 2022, along with adding updates to a further 24 previously published advisories. The volume of new advisories continues to grow month on month, albeit only slightly, following the slump during the summer period. However, as well as new advisories, we are still seeing a large number of updates published to existing advisories which 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 majority of the October advisories again remained low. Although this month we again saw one advisory given a criticality rating of 4, whilst six others were rated at 3.



Breakdown of Advisory Criticality for Previous 12 Months

Advisory Summary

As the charts above show the advisories this month were mostly given criticality ratings of Informational (1) or Low (2) when initially published, which follows the pattern for the last 12 months where more than two thirds of our advisories received the same ratings. 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 initial publication, so even though an advisory may concern a vulnerability rated as critical by the vendor we may deem it to only initially warrant a low rating, if for example there is no publicly available exploit. This is under constant monitoring however and subsequent updates will increase the reported criticality level as required if circumstances should change.

Some advisories of note this month are:

SIG-652349 - Highly critical vulnerability in FortiOS and FortiProxy

- Early warning about a highly critical vulnerability in FortiOS and FortiProxy, shared by Fortinet since Wednesday to a few selected partners including Orange Cyberdefense, has been leaked publicly. Tracked as CVE-2022-40684, this vulnerability allows an attacker to bypass authentication and execute arbitrary commands as an administrator.
- The flaw is currently discussed on the Internet, in particular since a Twitter user mentioned the confidential advanced notice in a non-responsible manner a few hours ago. Some information about this vulnerability have been removed from a specific Reddit thread, in an attempt to limit its visibility. Nevertheless, it is very likely that many cybercriminals will try to leverage it as soon as the vulnerability details are available, as an exploit could possibly be easy to develop.
- Fortinet has already patched this vulnerability in version FortiOS 7.0.7 and 7.2.2, and FortiProxy version 7.0.7 and 7.2.1 (but this latest one is not yet available). The vendor didn't mention in the advanced notice if the vulnerability is currently exploited or not.
- Our CERT Orange Cyberdefense experts have set a maximum CVSS score of 10 for now. However, this score could be lowered as soon as more information is released by the vendor. We recommend you to patch as soon as possible, and if not possible, disable remote administrators' access for publicly-exposed administration interfaces.
- As soon as we received the advanced warning, equipments managed for our clients by OCD were patched proactively by our teams thus will not be at risk.

SIG-655909 - Threat actors use several RCE vulnerabilities affecting Veeam Backup & Replication

- On October 24, CloudSEK researchers published a report on 3 vulnerabilities located in Veeam Backup & Replication and discovered earlier this year, which are currently exploited in the wild to deploy various ransomware. The first two vulnerabilities consisting of CVE-2022-26500, CVE-2022-26501 exist due to a lack of verification of access to API functions via port 9380. Using these security bugs, an attacker can form requests specifically and carry out them on TCP port 9380 (Distribution Service) in order to execute arbitrary code.
- The third, less critical, is tracked as CVE-2022-26504 and allows a remote and authenticated attacker to create specially crafted requests and send them to TCP port 8732 (Veeam.Backup.PSManager process) in order to execute arbitrary code and thus take control of the system. Nevertheless, it is important to note that this vulnerability is exploitable if and only if the application is configured with "System Center Virtual Machine Manager" (SCVMM).

- According to a tweet from PT SWARM, a private PoC is available. Nevertheless, due to its exploitation, it is likely an exploit is available as well in the wild (perhaps sold on underground marketplaces). Indeed, we notably discovered a GitHub repository named "veeam-creds", which includes files that decrypt accounts directly from Veeam's database and that are capable of retrieving stored credentials from Veeam, thus suggesting it is related to a ransomware activity. Furthermore, according to researchers, a malware named "Veeamp" was also observed in the wild, and is allegedly used by the Monti Ransomware and Yanluowang ransomware groups.

SIG-654567 - Unofficial patch released for a zero-day flaw in the Windows Mark of the Web security mechanism

- Usually Windows automatically adds MotW flags to all files downloaded from untrusted sources, including ones extracted from downloaded ZIP archives, using a special 'Zone.Id' alternate data stream. As a consequence, these MotW labels enable Windows, Microsoft Office, web browsers, and other applications to generate warnings displayed to the user explaining that opening the files could lead to dangerous behavior, such as malware being installed on the device.
- However, vulnerability analyst Will Dormann has discovered that ZIP archives were not properly adding MoTW flags to decompressed files. This is a major security issue as for example Smart App Control will only work on files with MotW flags and Microsoft Office only block macros by default in documents tagged with MoTW. A malicious actor could then deliver malicious Word or Excel documents in a downloaded ZIP that would not have their macros blocked or would escape the inspection by Smart App Control.
- Since it was reported to Microsoft back in July but was not patched, the vulnerability has been exploited in the wild. On October 17, 0patch released a free patch for the following affected Windows versions:
    - Windows 10 v1803 and later
    - Windows 7 with or without ESU
    - Windows Server 2022
    - Windows Server 2019
    - Windows Server 2016
    - Windows Server 2012
    - Windows Server 2012 R2
    - Windows Server 2008 R2 with or without ESU.
- As a reminder, this is an unofficial mitigation measure, that may be applied temporary till Microsoft releases an official patch.

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.

Wicus

Chaos in the Twitter-verse

The recent development at Twitter is not directly relevant to cybersecurity, at least not on the surface. The ham-fisted approach of the new owner of Twitter is detrimental to the platform's reputation. The aggressive layoffs and indecisiveness on how to implement new policies or platform features does not bode well. The tech sector in the US is starting to see severe job cuts, with Meta and Microsoft also announcing staff reductions.

The aggressive layoffs at Twitter combined with the push for profitability could put more pressure on internal teams to take shortcuts that may compromise integrity of systems at Twitter. Twitter had several teams dedicated to ensuring the platform is not abused by people to spread falsehoods or flame negative public discourse through hate speech and other defamatory narratives. Culling or closing these teams will result in Twitter facing yet another onslaught that may damage its brand even further.

The resignation of several executives including the Chief Information Security Officer raised many eyebrows. A former Twitter CISO, Peiter Zatko, raised concerns about the cybersecurity practices at Twitter. This was making the news even before Elon Musk took ownership of Twitter and ended up at the US Senate Judiciary Committee. The types of problems listed by Zatko are not things that are easily fixed and could be systemic in nature. For example, Zatko stated that staff had too much access to Twitter user information and that basic practices such as software updates were not followed.

Twitter and many other social media companies are relied on by many for information or news about world happenings and even local events. That is why it's important for social media platforms to provide safe and trustworthy content. Perhaps the idea that this type of service is free is rather strange, especially coming from Silicon Valley, but the truth is that many of these free services are subsidized through data mining and or advertising. This relies on an active user base that is linked to real people. Musk did point out he believes that Twitter's real user numbers are lower than claimed.

Users have already flocked to other platforms such as Mastodon. All these changes now allow for more potential problems, such as impersonation, more negative content, and potentially phishing. It is also unclear if these community driven platforms can stand up against the Internet trolls and other threats that Twitter had experience with. The schism created by the takeover of Twitter will create more problems for us all as we will now have to engage on more platforms and expose ourself to more potential threats.

The role that technology plays in our society is very prominent and contributes a lot to how we perceive the world. Undermining these platforms are easy, making

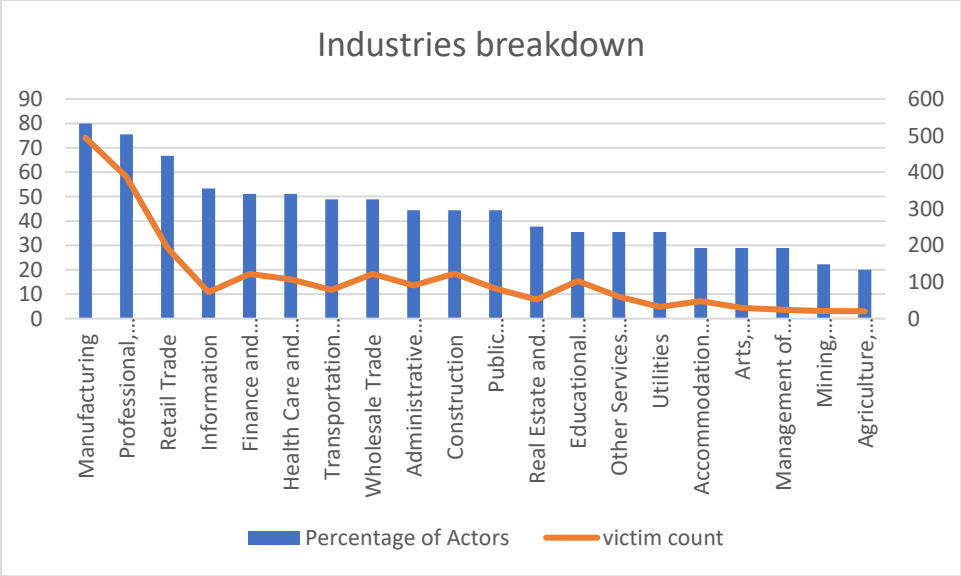
these platforms safe and trustworthy for users are difficult and requires dedicated skilled people.

Joshua

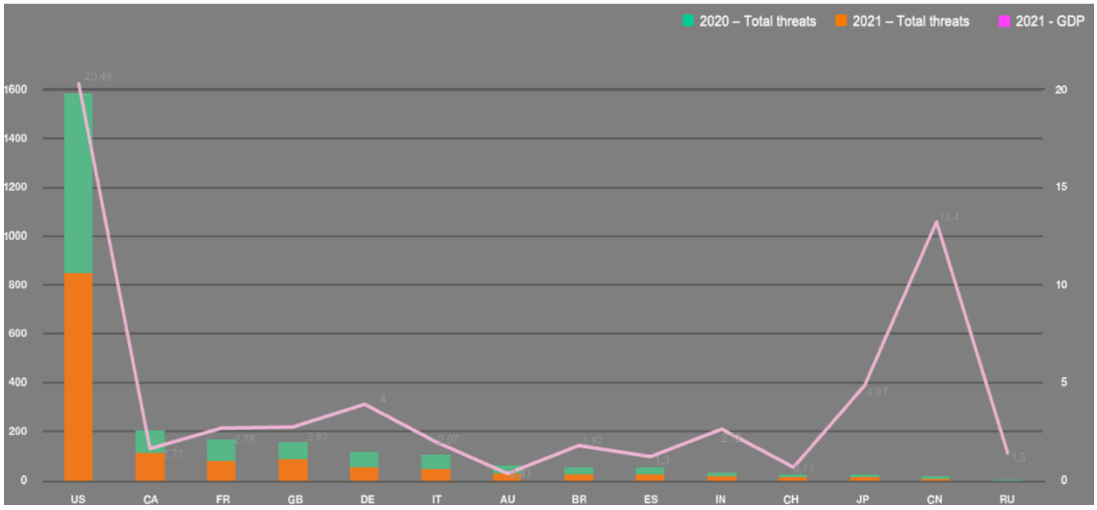
Victims of opportunity

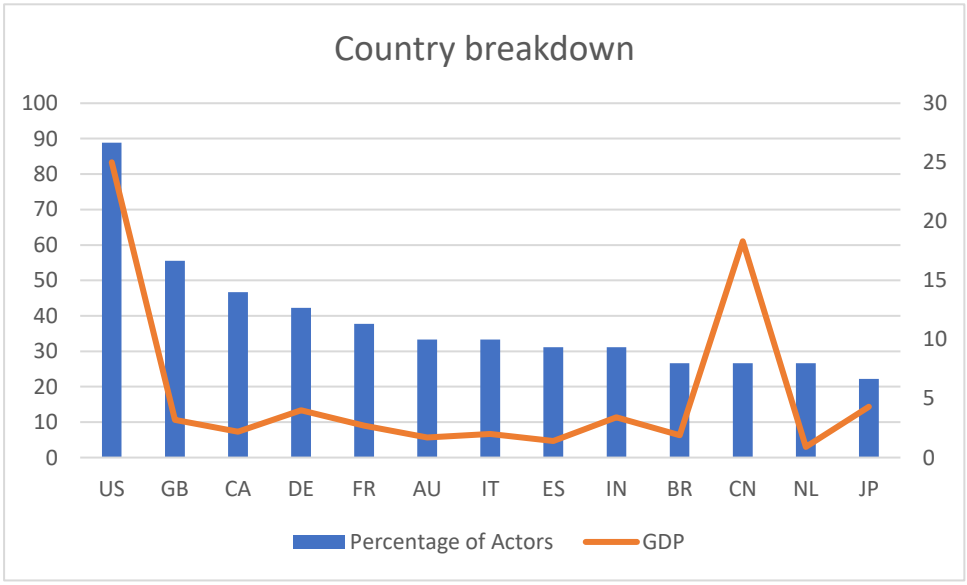
Cyber-Extortion is a massive problem and, with data showing a movement in activity from America to Europe, it is increasingly affecting people closer to home. When people look at statistics, such as the USA having the most victims, it does tend to lead people to believe this country is targeted the most and the same thing goes for the Manufacturing industry. We are here to explain this is not the case and we believe that Threat Actors are opportunistic and do not target per se.

The graph below shows data about double extortions collected over a year long time span from September ’21 till September ’22. It shows the percentage of Threat Actors we track that have attacked specific industries and shows the overall victim count collected for each Industry.



When we look at Industries, we generally see the overall victims for each industry but, another perspective rarely seen is the percentage of overall Threat Actors that have at least 1 victim in this industry. When looking at this it does not seem as extreme with a slow decline in Threat Actors targeting these industries. This shows that threat actors do not seem to target specific industries. This in addition with the fact that a subdivision in the Manufacturing industry has the highest government spending in the USA indicates that there are potentially more victims in this industry. The same thing occurs with the Professional, Scientific, and Technical Services where a subdivision of this receives the second highest government spending in the USA.





We also get the same results when we look at countries and compare the GDP of these countries. It shows clearly that most follow their GDP. There is one anomaly however, which is China, where their GDP is the second largest but in our data is only 13th in our ranking of the higher percentage of Actors having Victims in this country. This is a stark contrast to the graph showing the overall victim count and GDP where China is a greater outlier. This shows that Threat Actors are opportunistic and as you would expect the GDP is in close relation to the size of possible victims. There are many reasons for China being an outlier and whilst none can be confirmed as true, we do believe this is due to large language and cultural divides between the Threat Actors and China where they are generally avoided as it is seen as more effort for them to carry out attacks.

Overall, this data shows that Threat Actors do not target specific industries or countries, they generally use well known exploits that affect a large amount of people in search of easy victims that do not maintain up to date systems or have common misconfigurations. They use these to find any victims they can with no regard to who they will attack. It is a case of ‘attack now, think later’.

Good News Cyber

Cyber security firm Trellix posted a blog that they have proof that ransomware reward bounties linked to cybercrime are paying dividends. Trellix stated that they were able to facilitate the sharing of sensitive information provided by a REvil insider with law enforcement in exchange for a reward. This is unlike the CONTI leaks incident where the CONTI member leaked the information to the public for free due to the stance that CONTI leadership took to support Russia in the war with Ukraine.

A ransomware group going by the moniker Yanluowang had their internal chats leaked as well as information about the group's membership. Surprisingly the group gave the impression that they were Chinese, but from the leaks it is now clear they are Russian.

A member of the Netwalker ransomware crew was sentenced to 20 years in prison. The Canadian man forfeited $21.5 million as part of a plea agreement. Another Canadian man was arrested for his alleged involvement with the LockBit cyber extortion group. The LockBit man was later extradited to the U.S.

Interpol arrested 75 suspects allegedly with ties to the financial fraud cybercrime ring known as Black Axe. Operation Jackal was led by Interpol and included 14 law enforcement jurisdictions from Argentina, Australia, Côte d'Ivoire, France, Germany, Ireland, Italy, Malaysia, Nigeria, Spain, South Africa, the U.A.E, the U.K., and the U.S.

Another member of the infamous Lapsus$ group was arrested in Brazil. Little information is available about this. Several members of Lapsus$ were arrested throughout the year.

Dutch police were able to obtain 155 Deadbolt ransomware decryption keys for free by abusing a feature of the Bitcoin blockchain called 'zeroconf'. Bitcoin transactions need to be verified by the blockchain network before it can be considered official. This can take several minutes even hours in some cases. The recipient of the transaction can use zeroconf to assume that the transaction will be validated later, but the Dutch police cancelled the Bitcoin transaction instead. This edge case fooled the cyber criminals into releasing the keys thinking they were paid when they were in fact not.