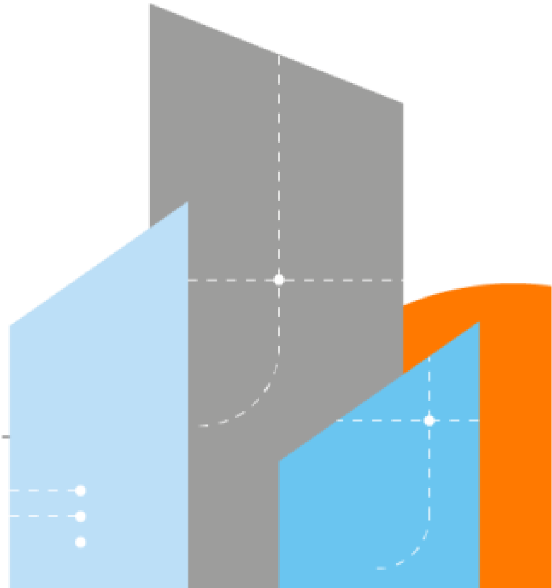
Orange
Cyberdefense

Security Intelligence

Monthly Report

July 2022



orange™

CONTENTS

INTRODUCTION

Welcome to the Security Research Center monthly report for July 2022. This is a return to the shorter format following the quarterly version of our report last month. We plan to extend and develop this report as we move forward, and work is still going on in the background to introduce new sections and to restore some of the statistical analysis we previously provided.

July seems to have been a relatively quiet month, especially in terms of the number of World Watch advisories we published. This is likely due to large parts of Europe taking summer vacations, as such we expect August to be similar and things to pick back up after that.

As we write we are in the middle of what is referred to as “Hacker Summer Camp”, with BSides, Black Hat USA & DEF CON all taking place in quick succession of one another in Las Vegas. We hope to be able to provide some summary of any interesting developments coming out of those conferences in our August report.

At a glance

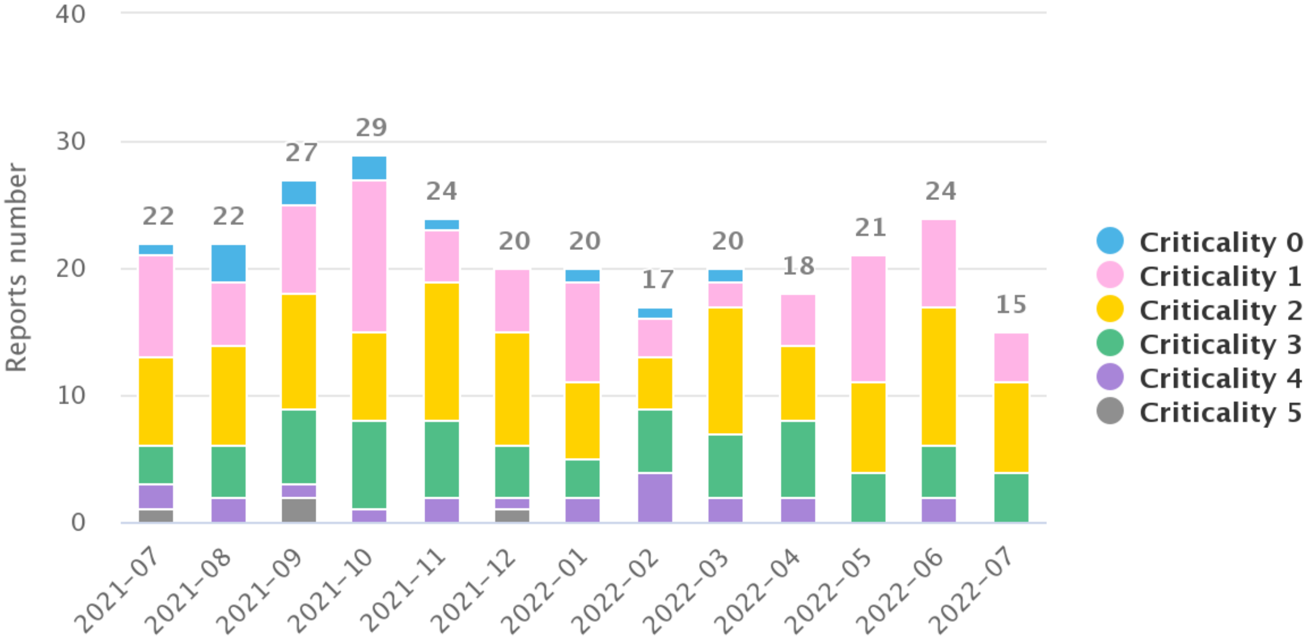
Orange Cyberdefense are proud to have been rated as a Leader in The Forrester Wave™: European Managed Security Services Providers, Q3 2022!

This is a great testament of our expertise, value-added services enriched by our proprietary intelligence and IP providing superior outcomes to organisations that rightly demand more than an alert factory from their MSSP.

You can download the report here: https://www.orangecyberdefense.com/uk/market-recognition/forrester

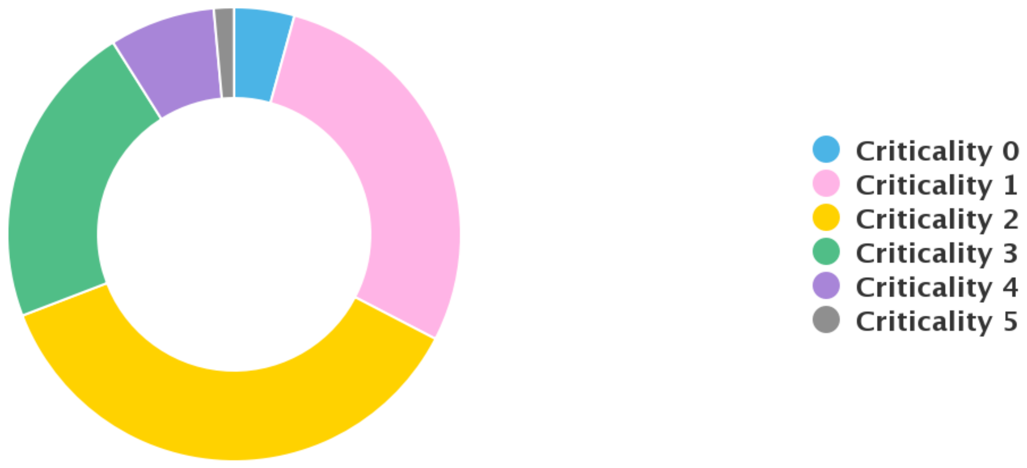
World Watch Review July 2022

The Orange Cyberdefense CERT published a total of 15 new World Watch advisories during July 2022, along with adding updates to a further 17 previously published advisories. This volume of new advisories is the lowest we have seen in the past 12 months; however, this is likely caused by a decline in activity generally, potentially caused by the summer period in Europe.



Breakdown of Published Advisories Previous 12 Months

Alongside the lower number of advisories, the criticality levels allocated to the July advisories again remained low. The highest allocated criticality was level 3, with only four 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-626545 - Raspberry Robin malware infects Windows networks with external drives

- Raspberry Robin is the name given by Red Canary to a malicious campaign involving compromised USB keys as the initial vector. These embed a malevolent ".lnk" (Windows shortcut) often masqueraded as a folder, that downloads additional obfuscated payloads whose final goal remains undetermined as of now. Indeed, no additional malicious activity was observed so far (for instance, no Cobalt Strike or other post-exploitation framework dropped).
- Updated 01/08/2022: In a tweet published on July 28, Microsoft's Security Intelligence team tied the recent Raspberry Robin USB-based worm attacks to Russian-speaking cybercrime syndicate EvilCorp. This discovery actually comes as an update to a previous report from Microsoft Threat Intelligence Center published on May 2022, in which researchers identified a partnership between EvilCorp (also tracked as UNC2165 by Mandiant or DEV-0243 by Microsoft) and an initial access broker called DEV-0206 by Microsoft (or UNC1543 by Mandiant and TA569 by ProofPoint). This second threat actor notably leverages a proprietary loader malware called FakeUpdates or SocGholish.

SIG-626589 - Red-Teaming tool Brute Ratel C4 increasingly leveraged by threat actors for post-exploitation

- A recent report from Unit 42 (Palo Alto) highlights how a red-teaming and adversarial attack simulation tool has been recently leveraged by threat actors potentially including APT29 (a.k.a. Nobelium), as well as other cybercrime threat actors. Named Brute Ratel C4 (BRc4), this tool has managed to stay out of the spotlight and to remain less known than its famous competitor, Cobalt Strike, even though it is no less sophisticated. Indeed, as researchers note, Brute Ratel was specifically designed to avoid detection by endpoint detection and response and antivirus capabilities. This is why related samples are currently often not detected by antivirus engines.

SIG-634107 - Microsoft details KNOTWEED, an Austrian company called DSIRF using zero-days to push their Subzero malware

- On July 27, Microsoft published a detailed report about a threat actor they called KNOTWEED which is in fact an Austrian company named DSIRF providing offensive services and products. This company has allegedly targeted European and Central American entities using their malware toolset dubbed Subzero. This arsenal leverages multiple Windows and Adobe 0-day exploits, including for one recently patched vulnerability (CVE-2022-22047). Microsoft believes DSIRF may have sold its toolset to third parties but has also used it to target victims directly as traces of its own infrastructure have been detected on different attacks.

SIG-629097 - Microsoft fixes an elevation of privilege vulnerability exploited in the wild

- New security updates have been released by Microsoft to fix 84 vulnerabilities, including 4 rated as critical and 80 important.
- Among these vulnerabilities, one of them is currently exploited in the wild: CVE-2022-22047. The latter is a local elevation of privilege bug in the Windows Client/Server Runtime Subsystem (CSRSS). If exploited, a local attacker can elevate his privileges as SYSTEM using unspecified vectors. CVE-2022-22047 received a maximum overall CVSS Score of 8.4 (out of 10) from our Vulnerability Intelligence Watch team.
- Unfortunately, Microsoft has not disclosed any technical information or information about potential attacks.

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.

Charl

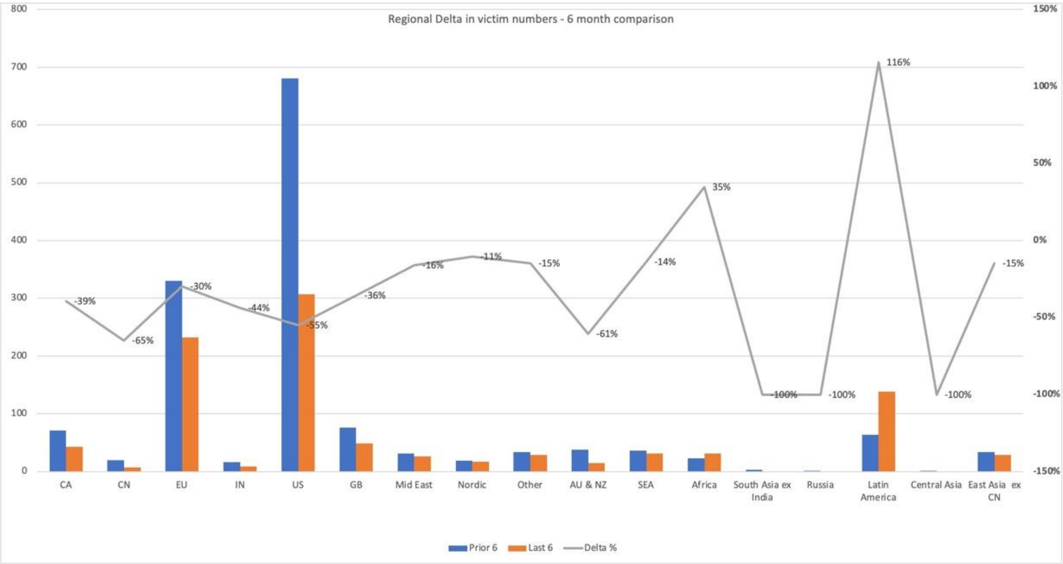
Cyber Extortion – Shifting tides

We've commented frequently in past about insights gleaned from data we collect on double extortion 'leak' sites. Recall that these are dark web sites hosted by dozens of cyber-criminal groups that use them to name and shame the victims of a compromise to extort a ransom from them. Because these sites are ultimately still 'public', we can find them and monitor them, providing us a unique ability to track the victims and thus gain insight into the crime.

The listing of a victim on such a leak site is the last stage of a complex chain of technical and criminal activity, with a multitude of moving parts, so the sites provide only a limited part of the whole picture. But due to their nature, the data they do provide is powerfully accurate and objective.

Using this data, we have long hypothesized that the demographics of cyber-extortion are slowly shifting. For two years now the victims have been predominantly located in large, western, and English-speaking countries. There are two reasons for this: Firstly, there are simply more businesses in large economies like the US, UK, Canada, and Germany. Targeting by the hackers behind Cyber Extortion is mostly opportunistic, so they acquire more victims where there are more potential victims to be had. Secondly, Cyber Extortion is a crime of extortion, and therefore requires a relationship to be established between the victim and the criminal. It's much simpler for criminals to do this in western countries that they understand and in the English language.

However, after almost three years of the double-extortion scourge, countries like the US, Canada and the UK are becoming less attractive to criminals. This is partially because of the political backlash caused by high profile compromises like Colonial Pipeline, and the Law Enforcement pressure that followed. It may also be because the 'market' for new victims is becoming saturated as security controls improve and more criminal actors enter the space. These two forms of pressure have been gradually causing criminals to seek out victims in new, less familiar geographies. The result of this shift can be seen in the chart below:



We assigned all countries to broader 'regions', then looked at the numbers for the 6 months ending July 22, compared with the 6 months prior to that.

Overall, the number of victims we're seeing via double-extortion leak sites has decreased by 35% between those two periods. But notice the variations from region to region – the grey line, Y-axis on the right. Note that 0% is somewhere in the middle of that Axis.

We see a 55% **decrease** in the US, 39% in Canada, 30% for Europe broadly, and 36% in the UK. BUT... we see an **increase** of 35% in African victims, and 116% in Latin America (albeit off low base).

A view of just the last 6 months tells basically the same story but is even more acute. In the last 3 months we've seen victim numbers increasing in the Middle East, staying constant in the Nordics, and slowing their decrease in India, compared to huge decreases in Canada, the US, Europe, and Great Britain.

The lesson to be taken from this data (if the trends hold true) is that Cyber Extortion is being driven by a set of inexorable technical, political, and economic forces, and will therefore not be fundamentally disrupted by simple, isolated interventions. We are dealing with a global problem, and we will need a global response to counter it. Allowing the problem to shift to less developed and non-anglophone countries may provide temporary relief in the developed west, but the overall impact on political stability, international supply chains and indeed the global economy will still be felt.

Cyber Extortion remains a very real and pressing concern both globally and locally, and we may not allow ourselves to rest for one minute in our collective and individual efforts to counter the systemic factors that drive this issue, or the specific crime that emerges as a symptom.

Wicus

Gone phishing!

Exploiting weaknesses in human nature that trick victims into performing actions that give the attacker access to the inside of a well defended space is as old as Greek mythology. Yet it remains one of the most effective forms of attack even in today’s high-tech world. Phishing, it seems, is perhaps easier than ever.

One would think that with all the technology and foresight we would be more protected from manipulation. Opening malicious attachments or being tricked in to giving credentials to a spoofed website is still one of the easiest ways for attackers to gain access to a company according to the Verizon DBIR 2022 report. The introduction of multi-factor authentication (MFA) is one way to block against credential theft, but attackers find ways to leverage known weaknesses such as authentication cookie theft. In turn phishing resistant MFA techniques exist but this is still less common than it ought to be.

The classic trojan email attachment seems to be still the simplest way into an organization, especially if the lure is well constructed. Recent news reports of successful phishing attacks linked to the Democratic People's Republic of Korea (DPRK), also known as North Korea, are a sobering reminder that we need to be almost suspicious of every email or direct message we get. These reports showed that North Korea continues to target businesses and individuals linked to cryptocurrencies and emptying the virtual “crypto coffers” are their main goal.

In one incident attackers sent an email with a malicious PDF attachment to a developer working for a company that specializes in monetizing non-fungible tokens (NFTs) through online gaming. These NFTs are linked to blockchain technologies that in turn represent some form of value. The attackers gained access to the developer’s machine when a malicious attachment was opened and proceeded to move laterally through the compromised environment. The attackers also used GitHub as the command-and-control center to hide in the background as this is a common website for developers to visit. The attackers allegedly managed to steal the equivalent of $617 million in blockchain currency.

There is an ongoing theme in that people specializing in developing solutions for blockchain technologies are being targeted through professional networking platforms such as LinkedIn. In fact, there was a report in July 2022 by Check Point claiming that LinkedIn was the number one impersonated brand in phishing lures. The phishing lures seek to recruit people into joining fake or spoofed companies. These lures then contain malicious attachments. Similarly, there have been reports of shady individuals applying for jobs at companies operating in the blockchain technology space with the intent of abusing their access once hired. Whether or not these attackers are joined up or working independently, the blockchain industry is being targeted heavily.

This does not mean that other industries are safe. Businesses should learn from what is happening in other industries and adopt procedures to block or detect potential manipulation early. The human is a point that requires regular reinforcement, but the judicious use of technology can help in reducing the risk to manageable levels.

Joshua

A Call for Clarity

LockBit has recently updated its capabilities to provide more functionality for their ransom attacks. Now, was I talking about the ransomware or their leak site?

The answer to that could be up for debate depending on how you interpreted that statement: I used it to highlight the overlap in ransom attacks and the extortion techniques involved. In modern attacks some of the threat actors, such as BlackBasta, do not fit the description of Ransom. Ransom is the definition of holding something of value from someone with a demand of money. This used to be the case where files were held at ransom, but we have seen a shift from this typical model to more inventive ways to extort victims, such as leaking files, and Lockbit's new feature that will leak the negotiation chat.

Both examples highlight the need for more descriptive language that does not become outdated over time. Many others, including myself, describe these attacks as 'cyber extortion'. The separation between the cyber-attack and then the cyber extortion afterwards needs to be clear as these both evolve separately. The former is a constant battle to out manoeuvre defences whereas the latter is based on a business model.

The cyber extortion techniques are not based on "what is the best way we can make them pay?" it is "what is the best way we can make them pay with a good ROI?". Most of the techniques we see are low cost for the attackers, such as leaking files so they could use the information stolen to leverage payments, but this is often avoided as the investment is not worth the reward. It is easier for them to spend that time finding a new victim to exploit. The opposite is true for the ransomware used to infect a system; it has a large number of resources put into it to keep it up to date with the SOTA.

Clearly the call for new language to understand the different elements of an attack is vital to decrease ambiguity and increase clarity to aid the transmission of information more effectively.

Good News Cyber

The No More Ransom initiative celebrates its 6-year anniversary in July 2022. Originally created by the National High Tech Crime Unit of the Netherland's police and Europol's European Cybercrime Centre, Kaspersky and McAfee. The project's goal is to help ransomware victims recover from a ransomware incident without having to pay the extortion money. The project has now grown and consists of over 188 partners from public and private sectors. The initiative provides free tooling to assist with recovery from 165 ransomware variants. The No More Ransom initiative originally was only available in English, but now boasts support for 37 languages and has helped over 1.5 million victims of ransomware.

The Maastricht University (UM), a Dutch university, was the victim of a ransomware attack in December 2019. The university paid the ransom at the time to recover from the incident. The original ransom amount paid by UM was 30 BTC, valued then at €197,000. The Dutch Public Prosecution Service (DDPS) managed to trace the crypto wallet linked to the incident and froze it. At the time the wallet contained €40,000 in Bitcoin. The value of Bitcoin increased substantially since the December 2019 incident and the content of the wallet is now said to be worth €500,000. The recovered amount at the new Bitcoin price is valued at double the original Euro linked ransomware payment amount. UM said the damaged caused by the December 2019 was immeasurable, but the recovered money will be put toward helping students that require financial assistance.

The US Justice department has managed to recover $500,000 of ransomware payments said to be destined for North Korea. Two healthcare institutions, one in Kansas and one in Colorado, made payments to the ransomware operators. At the same time the two victims reported the incidents to the FBI. The cooperation with the FBI resulted in the identification of the malware and the attribution of the attackers.

A Russian national, Alexander Vinnik, was found guilty in a French court. Mr Vinnik owned and operated a crypto currency exchange called BTC-e that was used by criminals to launder cryptocurrencies. Mr Vinnik was arrested in 2017 while on holiday in Greece, then extradited to France to face money laundering charges. Mr Vinnik was cleared of any involvement in running or operating ransomware. Mr Vinnik was held in French custody the past two years and was sent to Greece after being sentenced to five years in prison. Now Mr Vinnik has been extradited again, this time to the USA to face further charges.