
nccgroup
Cyber Threat Intelligence Report
November 2023

Contents

Introduction

Welcome to NCC Group's monthly Cyber Threat Intelligence Report, bringing you exclusive insight into the latest Threat Intelligence, updates on recent and emerging advances in the threat landscape and a deep understanding of the latest Tactics, Techniques and Procedures (TTPs) of threat actors.

Let us keep watch over the cyber and geopolitical landscape so you don't have to.

Take a look at our Cyber Threat Intelligence webpage to view all our previous reports and subscribe to our monthly highlights webinar.

Ransomware Tracking

We are continuing to track ransomware groups operating the hack and leak double extortion tactic, this is achieved by actively monitoring the leak sites used by each ransomware group and scraping victim details as they are released.

By recording this data and classifying the victims by sector, we are able to derive additional insights such as, which sectors are being targeted this month, and how do these insights compare to previous months?

November attacks

442

Month on month

+30%

Analyst Comments

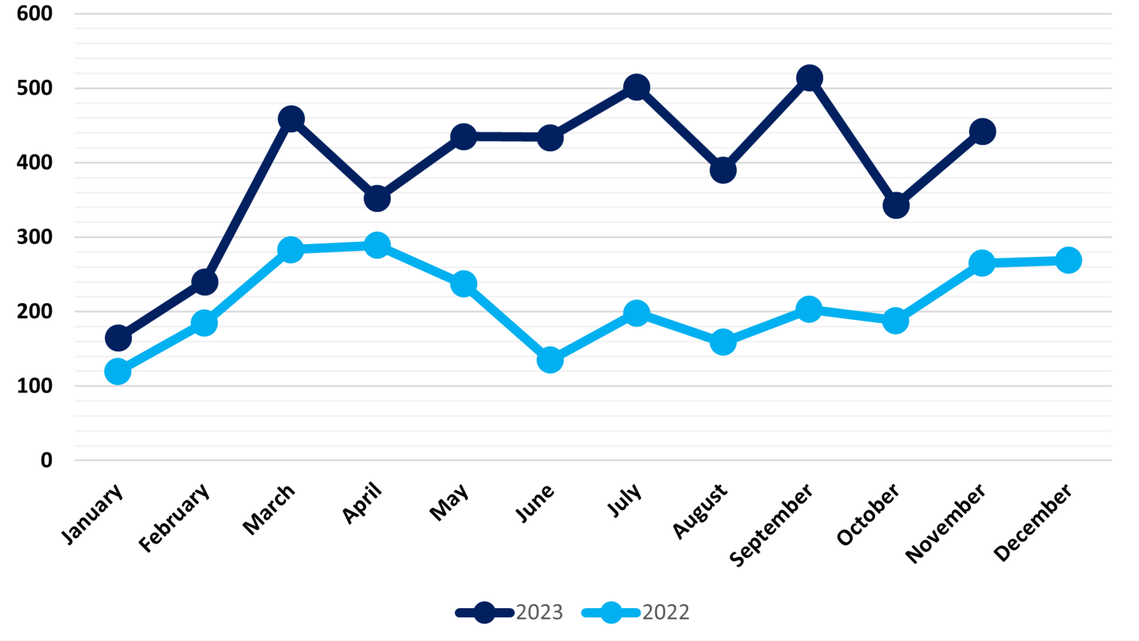

Figure 1: Global Ransomware Attacks by Month 2022 - 2023

fter the significant drop in observed ransomware attacks from September to October, November has seen numbers rebound more to where we would expect them to be. From 341 cases in October jumping 30% to a total of 442, November 2023 observed 67% more incidents than during the same period last year. Though not as high of a year-over-year increase as October, this most certainly matches the trend set by every other month in 2023 so far.

With the return to form in November, we have now met and surpassed the prediction of observing 4,000 ransomware incidents in 2023. So far, with December still to go, NCC Group has reported on a total of 4,276 observed incidents. This is less than 1000 incidents fewer than the total for 2021 and 2022 combined (5,198) and goes to show by just how much the global ransomware scene has exploded in the last year.

Sectors

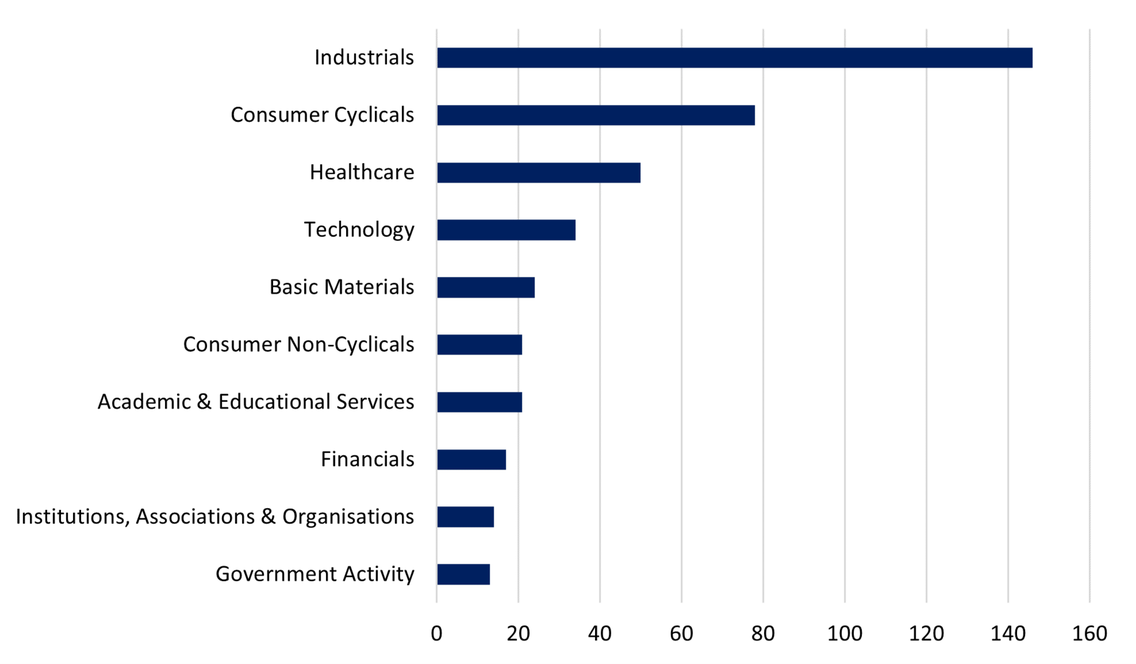

Figure 2: Top 10 Sectors Targeted in November 2023

In the last Threat Pulse we noted that (for the first time since February 2023) there was a change from the top three most targeted sectors being the usual Industrials, Consumer Cyclicals and Technology, where Healthcare took third place. While it would have been entirely expected activity to see this shift back to the usual most targeted sectors, the results show that Healthcare has in fact retained its third-place position, connoting a more concrete shift in the ransomware hack and leak threat landscape. Regardless, Industrials continues to be the most targeted sector with 146 cases within (accounting for the usual 33% of all attacks) which is a 28% increase from October's 114.

The Industrials sector will likely continue to be the most targeted sector for a number of reasons. These include the breadth and diversity of organisations existing within, the nature of them as many store vast quantities of either Personally Identifiable Information (PII) or Intellectual Property (IP) if not both, and the potentially expanded attack surface due to Information Technology / Operational Technology (IT/OT) convergence. Although there have been shifts in the top three this month, NCC Group do not foresee Industrials shifting from first place due to the reasons presented above.

Also following the usual pattern is Consumer Cyclicals with the second highest number of attacks for November. This month it experienced 78 attacks compared to the 56 in October which represents a 39% increase month-on-month, bringing it closer to its previous totals.

Finally, as mentioned, Healthcare has maintained its position as third-most targeted in an unexpected threat landscape shift. In October the sector experienced 33 attacks and, when compared with the 50 attacks that have been recorded in November, this marks a 52% increase month-on-month. NCC Group will continue to monitor the activity within this sector to see if it continues into the New Year.

Threat Actors

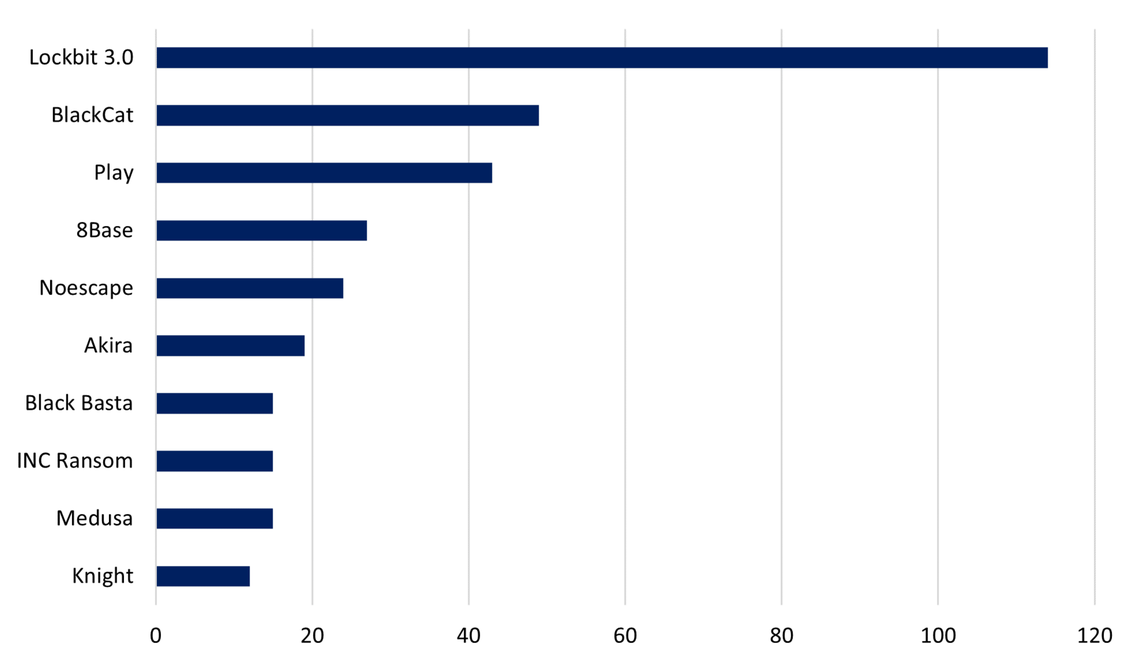

Figure 3: Top 10 Threat Actors November 2023

The month of November brings the third highest activity recorded in 2023 so far with the total number of attacks being 442, which represents a month-on-month increase of 29% from 343 attacks recorded in October. The other two months with record breaking activity this year were September with 514 attacks and July with 502 attacks. This month, the top three; LockBit, BlackCat and Play jointly contribute 47% (or 206 attacks) of the monthly total. Further details on the top three activity are available in the following pages.

8Base is fourth with 27 attacks, or 6% of the monthly total, which is a 29% increase on October's figure which was 21 attacks. The group has not been this close to the top three since August when they ranked third with a total of 32 attacks. Recent findings from Cisco Talos highlight that 8Base utilises Phobos ransomware to conduct their attacks. Phobos was initially identified in 2018 as a successor to the Dharma malware family and as a result of its simplistic design, the strain became quite popular with threat actors of varying technical abilities. Cisco Talos' findings could mean that either the 8Base's origins are related to Phobos or that the group prefers to rely on already existing ransomware strains for ease. The only notable difference that was identified between 8Base's Phobos variant and other existing samples was that 8Base's Phobos payload incorporates an embedded configuration.

Noescape is fifth with 24 attacks, or 5% of the monthly total, which also indicates a 29% decrease on last month's figure. The month of October marked the highest level of activity recorded for the group in NCC Group's database which was 34 attacks. What is currently known about the group is that it is believed to be a successor of Avaddon, which was a ransomware operation that shut down in 2021. Noescape first appeared to the scene in June 2023, targeting businesses across the Industrials' sector via double-extortion attacks. Since June, what we have observed in our data is that the group seems to favour businesses in the Industrials and Consumer Cyclicals' sectors as their top targets. In fact, 54% (13 attacks) of November's activity falls within these two sectors with Professional & Commercial Services (3 attacks) and Homebuilding & Construction Supplies (2 attacks) being the most targeted industries within these sectors.

Our Cyber Incident Response Team (CIRT) team released an article shedding some light on the group's Tactics, Techniques and Procedures (TTPs) following a recent incident response engagement. What the team observed during the engagement was that the threat actor gained initial access via exploiting a publicly facing Microsoft Exchange server which then led to the creation of webshells in order to gain an initial foothold into the victim's environment. The team also concluded that the threat actor seemed to be quite noisy in their approach, due to the deployment of various different tools when trying to disable antivirus as well as dump credentials; something that would not usually be the case with a more experienced threat actor. A further access method was observed as a back-up option in case the initial access vector ended up being closed. Finally, data exfiltration took place, which resulted in being interrupted due to the premature ransomware execution. Further details identified during the engagement are available here.

Regions

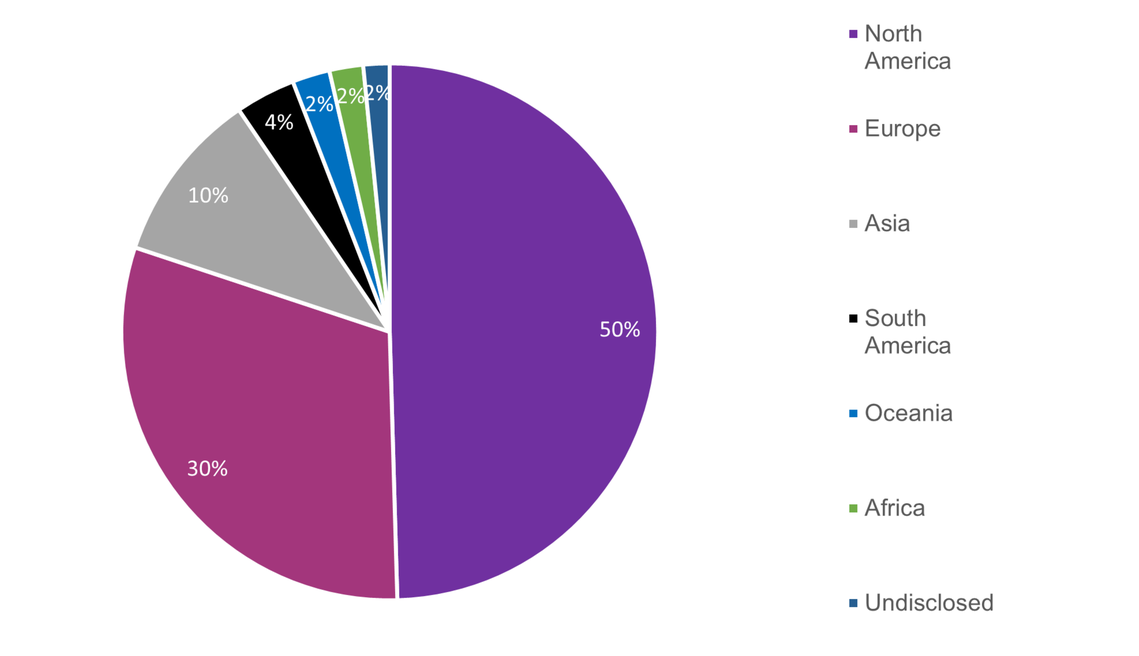

Figure 4: Regional Analysis November 2023

As is expected, North America and Europe observed the overwhelming majority of all ransomware attacks in November. There was a 29% increase of overall attacks from October to November, though this increase still falls short of the scale of attacks observed in September and subsequently, the breakdown of attacks per region are still lower as well.

North America observed 219 attacks, representing 50% of the total of 442 seen globally throughout November. This is an increase of 49 attacks from what was witnessed in October, or a proportional increase of 27%. Europe witnessed a total of 135 attacks in November, an increase of 36 attacks over October's 99, representing a 36% month on month increase. This proportional increase is greater than the overall month on month increase for all global attacks, however, should not be taken as indicative of a shifting focus for TAs from North America to Europe after only one month.

Asia is again the third-most targeted region, observing 46 attacks in November. This is an increase of 11 attacks from the 35 it experienced in October, an increase of 31%. South America, Oceania, and Africa are once again fourth-, fifth-, and sixth-most targeted with 16, 10, and 9 attacks respectively. What does stand out is the increase in attacks on undisclosed targets, and therefore undisclosed regions. In October there were a total of 3 of these attacks, whilst November has 7. These are listed on the leak sites of ransomware operators, but with some details obfuscated; a tactic, often used by BianLian though increasingly by other actors as well, to apply pressure to an organisation to pay a ransom before revealing all of their details.

Threat Spotlight

Return of Carbanak

This month our readers are in for a double treat from a double threat. Our tactical analysts have observed a new malicious campaign, employing both a previously undiscovered .NET loader, as well as, surprisingly, a Carbanak payload.

Old friends and old trends

Carbanak is a well-known banking malware that emerged around 2014 as a tool for infiltrating financial systems; the name refers both to the tool itself and to the campaigns it was used in. Its operators employed advanced phishing techniques to compromise bank employees, gaining access to internal networks through human entry points, and deploying the remote backdoor. From there, criminals gunned straight for taking control of the payment processing services.

Over the years, Carbanak evolved by incorporating various attack vectors and techniques to diversify their effectiveness, including manipulating ATM software and altering bank databases to inflate balance. Its popularity – or at the very least, visibility – decreased significantly in recent years. The most notable occurrences of Carbanak being used in the 2020s are attributed to FIN7, a famous Russian APT group responsible for billion-dollar attacks, as well as ALPHV ransomware-as-a-service scheme. That is, until last month.

2023: Carbanback on track

While the pre-emptive consensus of our analysts is that the core malware remains largely unchanged, the return of Carbanak is heralded by a new distribution chain with the help of new .NET friends.

The malware is distributed through compromised websites, storing malicious .msi payloads in inconspicuous /download/ paths. The distributed MSI files are impersonating various business-related software. Imposters include, among others, a CRM platform HubSpot, a data management software Veeam, and the accounting tool Xero.

nccgroup

Our experts are here to help you every step of the way. Contact us today to learn more about cyber security.