nccgroup

Cyber Threat Intelligence Report

6 month review

January - June 2023

Contents

Introduction

At the beginning of the year, we reported on a reduction in the volume and monetary impact of ransomware cases in 2022 compared to 2021 in the light of law enforcement interventions. However, we urged caution, that the war against ransomware was not yet won. What we have seen, is record numbers of victims of cyber-criminal groups deploying ransomware and operating double-extortion techniques.

In the first half of this year, we have witnessed a 67% increase compared to the same period in 2022, with a total of 2085 incidents recorded by our Cyber Threat Intelligence Team. This is a staggering increase, and record numbers since NCC Group started monitoring ransomware victim numbers in 2020. This increase has in no small part been heavily influenced by the increasing numbers of RaaS operators and the ever-evolving ransomware/data exfiltration business model.

We have also been monitoring increased activity and number of Initial Access Brokers (IAB's) operating across criminal forums and marketplaces on the dark web. As IABs facilitate many further criminal activities, from ransomware, to shop scams, to exploiting POS terminals, their roles are becoming more specialised and segmented along with the rest of the underground cyber-crime economy.

February marked a year since the invasion of Ukraine by Russia. At the time of the invasion, we provided details of the prevalence of wiper malware which was of concern to organisations around the globe. We also reported on the likelihood of increased hacktivist activity by both Ukrainian and Russian supporters. During the first half of the year, it is this hacktivist activity that has been most prevalent, particularly from the pro-Russian group 'Killnet' and their affiliates such as 'Anonymous Sudan'.

With relatively low-impact DDoS campaigns, Killnet has repeatedly targeted public services and critical national infrastructure of Western Nations that have provided support to Ukraine. What we have noted however is that the Group's capabilities behind their volumetric attacks have improved, and larger more mature organisations are having operations disrupted. It is likely that we will see this trend continuing in the second half of the year.

Threat actors have again been able to take advantage of critical vulnerabilities in widely used software. This has been especially impactful in the ransomware/data extortion world, where CloP have impacted hundreds of organisations having exploited two file management platforms, MOVEit and GoAnywhere. Adding to the impact of supply chain compromises, North Korean affiliated group 'Lazarus' have also had significant success and have created headaches for organisations around the world that use the 3CX telephony system.

It would also be remis not to touch on the growing impact of Artificial Intelligence, in particular the use of language-models such as ChatGPT, and AI Voice and image technology. In the latter case, we have seen evidence of criminal groups and nation state actors making use of deepfake technologies as part of social engineering campaigns and the generation of believable emails and other documentation using the likes of ChatGPT.

Key Events

3CX Supply Chain Attack

The 3CX supply chain attack demonstrated how threat actors continue to reap the benefits of this attack type and its extended reach. Notably, the incident manifested as a result of a previous supply chain breach enabling the criminals to compromise the 3CX network, underscoring the prolific and effective nature of this attack method. Notably, this has also been recorded as the world's first double supply chain attack, with one leading to the other, and may set the tone for future supply chain attacks.

3CX provides enterprise software to organisations, with features including chat, video and voice calls. A trojanised version of 3CX DesktopApp spread by North Koreas' Lazarus in March however, threated the security of its 600,000+ companies globally. Access to 3CX was enabled following Lazarus' initial compromise of financial software firm Trading Technologies, whose app was installed on the device of a 3CX employee, and from which threat actors were able to pivot.

Both financial gain and intelligence gathering were identified as the objectives, with targets spanning from CNI to financial trading. The attack stresses the breadth of victims that can be reached in a successful supply chain breach and by consequence, the widespread damage. Supply chains will remain the Achilles heel of many organisations if they do not ensure both the security of their own networks, as well as that of their respective partners.

Vulnerabilities Exploited: GoAnywhere, PaperCut and MOVEit

In the first half of 2023, threat actors continued to target and exploit zero-day vulnerabilities in major software packages, impacting their respective supply chains. Notably, a particular focus by ransomware actors to exploit vulnerabilities in public facing applications as an initial access method to support their wider operations was evidenced by Cl0p in 1H 2023.

GoAnywhere: On the 1st February 2023, a Remote Code Injection exploit was identified in Fortra GoAnywhere MFT, CVE-2023-0669, leading to its mass exploitation, notably by ransomware actors. Cl0p are known to have widely exploited this vulnerability, with their ransomware numbers rising from no targets in February to 129 in March.

PaperCut Vulnerability: Microsoft security researchers linked LockBit and Clop to April's attacks on PaperCut servers. Two vulnerabilities, CVE-2023-27350 and CVE-2023-27351 enable remote code authentication and information disclosure. On April 19th, the company disclosed its being exploited in the wild, with Lockbit and Cl0p named in attempts to steal corporate data from vulnerable servers. Additional attackers were also suspected of installing remote control software with an estimated 1,800 internet-facing servers that had been targeted. Notably, the attacks followed the release of patches in March, stressing the importance of timeliness when applying mitigations.

MOVEit: In May, the mass exploitation of a zero-day vulnerability in Progress Software's MOVEit Managed File Transfer package, a package used to support file and data exchange in organisations, prompted a global rise in ransomware activity. Notably, Cl0p sought to capitalise on the vulnerability, now tracked as CVE-2023-43362, to access and exfiltrate data resulting in a long-list of global victims. These victims are likely reflected in Cl0ps June statistics, with a major jump from 2-90 cases. This is the third critical vulnerability exploited to facilitate ransomware activity by the group after GoAnywhere and PaperCut.

Summary: With several operations of the like so close together, this may reflect a shift in initial access tactics and techniques for ransomware actors, with a greater focus on 'exploitation of a publicly facing application'. Notably, Cl0ps involvement in the compromise of three major vulnerabilities, and LockBit in PaperCut. In light of the group's successes, we might observe a greater number of ransomware actors incorporating this tactic into their arsenal in the future. Certainly, the benefits are reflected by Cl0ps success, who only conducted 42 attacks in 1H 2022, versus, 229 in 1H 2023, likely facilitated by vulnerability exploitation.

The Rise of Business Email Compromise

Microsoft Threat Intelligence reveals that Business Email Compromise remains a cause for concern into 1H 2023, findings across the April 2022-2023 period having identified an "alarming surge" in BEC attacks. On average, 156,000 daily BEC attempts, and an overall 38% increase in cyber-crime-as-a-service targeting business emails from 2019-2022. BEC attacks have always been a concern across the cyber threat landscape, and given this recent increase, NCC Group continues to perceive this as a prominent threat.

In addition, threat actors remain creative, advancing their methods where employing the use of malware-as-a-service (MaaS) platforms, such as BulletProftLink, to create industrial-scale malicious email campaigns. Such platforms offer up templates, hosting and automated services, which facilitates the broader BEC campaign. Ultimately, this extends a threat actors reach, increasing the number of potential compromises and profits.

The financial impact of BEC remains significant, with potential losses of over $590 million identified by the FBIs Recovery Asset Team via their Financial Fraud Kill Chain when assessing 2,838 BEC complaints involving domestic transactions. NCC Group recommend all organisations remain aware of the threat posed by BEC into 2H 2023, with continued phishing awareness as well as MaaS platforms exploited. Multi-Factor Authentication (MFA) should also be implemented, and businesses could consider anti-phishing infrastructure such as Secure Email Gateways (SEG) to further mitigate the threat.

Ransomware

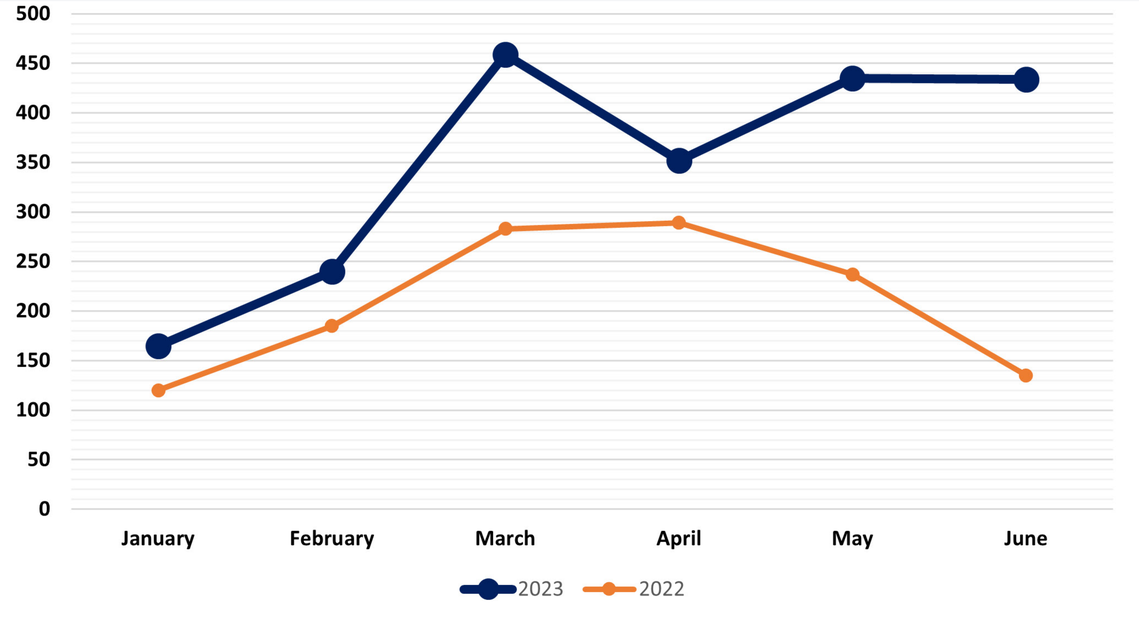

Figure 1 - Number of Hack and Leak Cases 1H 2022 - 1H 2023

1H 2023 observed 2085 incidents representing a 67% percentage increase from 1H 2022, in which 1249 incidents were recorded. This dramatic rise in ransomware numbers reflects the highest number of hack and leak cases ever recorded for a 6-month period in our database, which covers attacks from 2021 onwards. As predicted, the ransomware threat persists however; we did not quite anticipate the scale at which these attacks numbers would grow.

This boom can in part be attributed to the innovative approach ransomware actors employ. Notably, the widely discussed exploitation of the GoAnywhere vulnerability by Cl0p, largely responsible for March's high numbers (459), the greatest number of attacks observed for any given month in our database. Threat actors remained creative in April/May, in which Cl0p and LockBit 3.0 exploited the PaperCut and MOVEit vulnerability, contributing to a high number of victims in April (352), May (435), and rolling into June (434).

This 6-month period reveals how ransomware actors are perhaps more motivated than ever in their mission to target, breach and extort victims. With 2085 attacks in 1H 2023 alone, the data suggests that 2023 overall will see the highest attack numbers for 2021 -2023, already sitting closely behind the total annual figures for 2021 (2667) and 2022 (2531).

Sectors and Threat Actors

Although the overall attack numbers increased, the top sectors targeted remained unchanged. Industrials (663), Consumer Cyclicals (258) and Technology (238) continue to withstand the worst of attacks in 1H 2023, with numbers up from 1H 2022; Industrials (417), Consumer Cyclicals (259), Technology (117); Consumer Cyclicals remains almost equal.

Overall, this serves as an ongoing reminder to organisations within these sectors to reinforce ransomware defence measures, with particular emphasis on LockBit 3.0, who were responsible for the greatest number of attacks in each of these sectors during 1H 2022 and 2023. Defence should also focus on Lockbit 3.0 more broadly, as the threat landscape's most prolific threat actor. In 1H 2023, LockBit 3.0 were responsible for 523 ransomware attacks, up 11% from 468 in 1H 2022. Given that the group conducted 846 in 2022 overall, it is highly plausible that the group will overtake last year's numbers, with 6-months left to the year and a prolific affiliate scheme to support ransomware propagation.

DDoS

3CX Supply Chain Attack

Over the course of the last six months, Hacktivist groups such as the Russian-aligned Killnet have exemplified the alarming potential of politically motivated hackers within the ever-evolving cybersecurity landscape. Their activities have, and continue to pose a threat to governments, public services, and critical infrastructures, with the intent to disrupt, destabilise, and compromise sensitive systems.

In January, Killnet demonstrated their continued allegiance to Russia, threatening DDoS attacks against sectors in opposing nations. Notably, the Health Sector Cybersecurity Coordination Centre warned of an active DDoS risk, following the publication of global healthcare targets listed by the pro-Russian hacktivist group. The campaign however was reportedly launched in response to Biden's decision to send Abrams tanks to Ukraine, highlighting Killnet's alignment with Russia. These attacks spread to other NATO countries and sectors such as Government Activity. In this respect, cyber continues to play a role in the ongoing war, albeit not the cyberwarfare first anticipated. Rather, a secondary tool to conventional military tactics.

With geopolitical tensions still heightened due to the war in Ukraine, North Korea operating in ways that are broadly opposed by the international community, tensions in the Middle East and China, it is imperative for nations and enterprises to bolster their cyber defences, enhance threat intelligence sharing, and foster cross-border collaboration to counter the sophisticated tactics employed by these politically driven adversaries.

About DDoS attacks

Distributed Denial of Service (DDoS) attacks are a formidable weapon in the arsenal of cybercriminals that are evolving in size, frequency, and sophistication. They're capable of bringing all communication in a network to a halt, and with the increasing interconnectedness of devices their impact is growing in prevalence. This is demonstrated by the potential breadth of organisations that these threat actors claim to have impacted in this single offensive.

As the scale and complexity of these attacks continue to surge, it is imperative for businesses to fortify their defences, foster collaboration across sectors, and invest in robust mitigation strategies to safeguard their digital infrastructure from the disruptive and damaging effects of DDoS assaults. These types of attacks aren't going away any time soon and will keep being the preferred attack type for many malicious actors.

Advice for organisations impacted by a DDoS attack

Organisations aiming to safeguard themselves against DDoS attacks should place utmost importance on proactive defence measures to protect their digital assets. This includes developing incident response plans, conducting regular drills, and fostering collaboration with industry partners to stay abreast of emerging DDoS attack trends and mitigation techniques.

At a more granular level, it is crucial to establish a robust network infrastructure with ample bandwidth capacity capable of withstanding large-scale volumetric attacks. Traffic monitoring and anomaly detection systems can also enable prompt identification and mitigation of DDoS threats, minimising the impact on operations.

Conclusion

Based on what we have seen in the first half of the year, the key focus for organisations moving forward should be ensuring that cyber security fundamentals are addressed.

Based on the activities of Nation States, Cyber Criminals and Hacktivist Groups, it is clear that despite their technical capabilities, they continue to have great success taking advantage of more simplistic attack paths such as social engineering (phishing), poor password management, and unpatched applications and internet facing infrastructure.

While these initial access mechanisms are relatively simplistic, it is accepted that it can be challenging to manage. They often require cultural changes and rely on awareness of people within the organisation (for example to spot a phishing email, or to manage passwords appropriately). As such, it is highly recommended that organisations also focus on having a robust incident response plan, to help prepare for the potential of an attack being successful.

We have also touched on the fact that it is likely that certain organisations could appear in the crosshairs of certain hacktivist groups who are increasing their capabilities, but still rely heavily on high-volume Distributed Denial of Service Attacks. These attacks, as we know are typically short-lived and low-impact, but with increasing ‘strength’, they represent an increasing threat to organisations whose operations and internet facing applications are particularly sensitive to down-time.

nccgroup

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