Q4 2023 Quarterly Statement

Executive Summary – Q4 and the State of Cyber Throughout 2023

Throughout 2023 we have observed over 4,000 successful ransomware attacks, multiple new groups emerge, various evolutions in malware tactics and deployment, and multiple intrusion incidents.

Q1 saw the vulnerability in the 3CX Desktop Application under CVE-2023-29059. This was the first major supply chain attack of 2023 and unsurprisingly was not the last.

Exploitation of unpatched systems has been a common trend for multiple years and will continue to create easy wins for ransomware groups.

The most prevalent countries that were targeted were based in North America and Europe. This was later attributed to an alleged North Korean nexus and, a week later; multiple cryptocurrency companies were targeted by a malware strain known to be in use by the Lazarus group, dubbed Gopuram; which is evidence of the North Korean claim.

In Q2 we observed Cl0p take responsibility for the mass exploitation of the vulnerability in MoveIt across compromised systems. (CVE-2023-34362). During the initial exploitation over the first weekend, approximately 200 organizations were compromised. Today, that figure is over 2,000 organizations, with over 60 million individuals being affected as a result.

This attack led into major supply chain compromises further downstream for affected organizations and should serve as an early indicator of a critical vector for 2024. Furthering this point, exploitation of unpatched systems has been a common trend for multiple years and will continue to create easy wins for ransomware groups. Organizations should make efforts to audit and understand their third-party vendors to prevent becoming victim to supply chain attacks in 2024.

DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE.

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

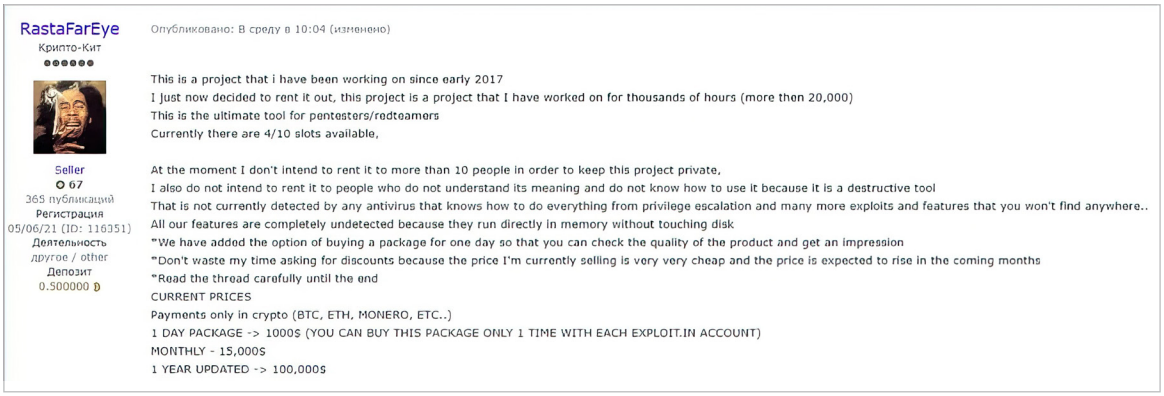
FRIENDLY CLOP.

PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.

Screenshot from Cl0ps Dark Web page

Q3 saw a major ransomware attack on the MGM group. The attack curiously was claimed by two separate threat actors, AlphV and the Scattered Spider groups. It is currently unclear whether they were working together at various stages of the operation. The AlphV group saw a 400% increase in their ransomware operations during this same time. This was likely the catalyst for the FBI stepping in during our Q4 observations, which we will cover later in this report.

An existing malware strain dubbed DarkGate has changed its tactics of delivery with devastating results. The malware author switched to advertising the strain on darkweb forums and offer it out on a Malware as a Service (Maas) model, for use by other threat actors. The CyberMaxx team has personally identified multiple true positive compromises as a result.



Darkgate malware listing on Dark Web Forum

Our tracking of high impact groups had shown that their activity continues to grow quarter-over-quarter. These are opportunistic threat actors that have previously mobilized high severity vulnerabilities in the past within hours, targeting organizations that were slow to patch.

DarkGate is a loader malware that has been used to infect a system with various utilities, including infostealers, follow-up payloads and ransomware. Until very recently, Darkgate was distributed through phishing emails however since June 16, 2023, the developer (known as RastaFarEye) has been advertising DarkGate on darkweb forums, offering it as a service. Due to this, we have witnessed firsthand a sharp increase in the frequency of infections, alongside finding multiple true positive infections during our IR efforts.

More details on the various loading techniques can be found at the CyberMaxx Blog Post titled Darkgate Malware: Initial Loaders and How to Mitigate Issues.

Most recently across Q4 we observed the FBI seize AlphV's website, which was promptly taken back by the ransomware gang – this cycle repeated approximately four times before concluding. During the seizures Lockbit allegedly reached out to several high ranking AlphV developers and affiliates. We will see if Lockbit's modus operandi changes in 2024 as a result of this rumored strategic acquisition.

Definition of Loader Malware

Loader malware is designed to serve several functions within the attacker killchain. Loader malware serves two main purposes:

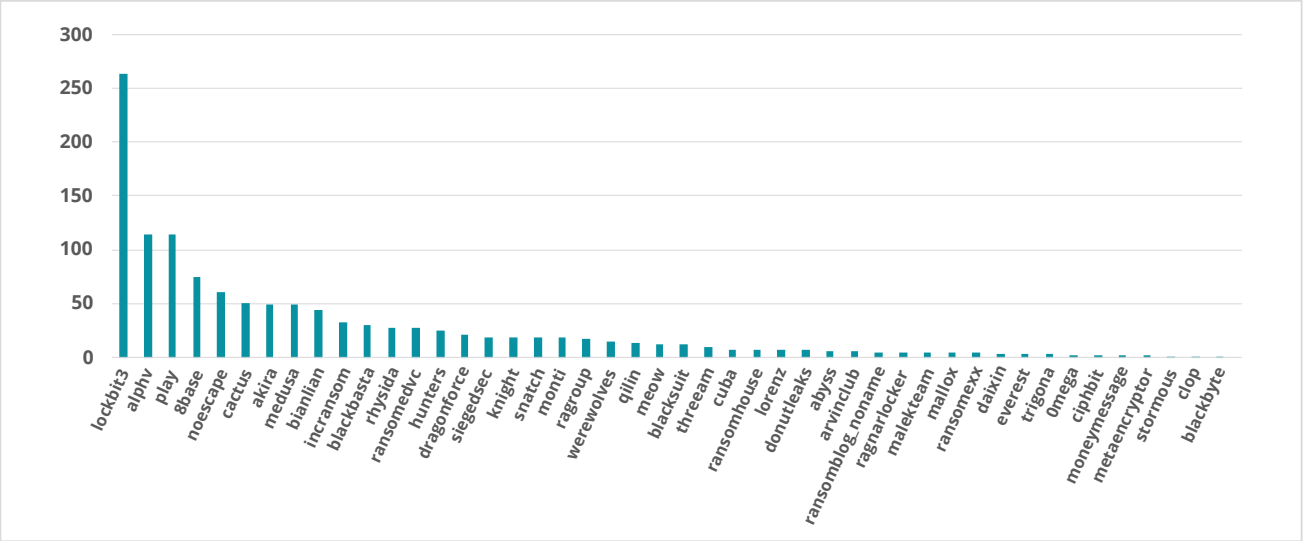
- Set up the target system to increase the likelihood of successful infection
- Test that the environment is suitable for the later payload to execute correctly. This includes testing for debuggers, virtual environments, and other monitoring / testing sandboxes

The above strategies are designed to stop defenders from accessing their payload for reverse-engineering and defensive efforts. By testing the environment first, the likelihood of successful execution increases significantly.

There can be multiple payloads in a loader chain. It is not uncommon to see first, second, third and fourth stage payloads all that perform some different task or requirement for the final infection stage.

So what is the final stage payload? The answer to that is it depends. Loader malware is usually bundled with several features, which typically allow the strain to be modular and load multiple different items that an attack may require. These range from ransomware directly to RAT, Infostealers, crypto-miners, and many others. Loader malwares focus is to increase the success of the later payload.

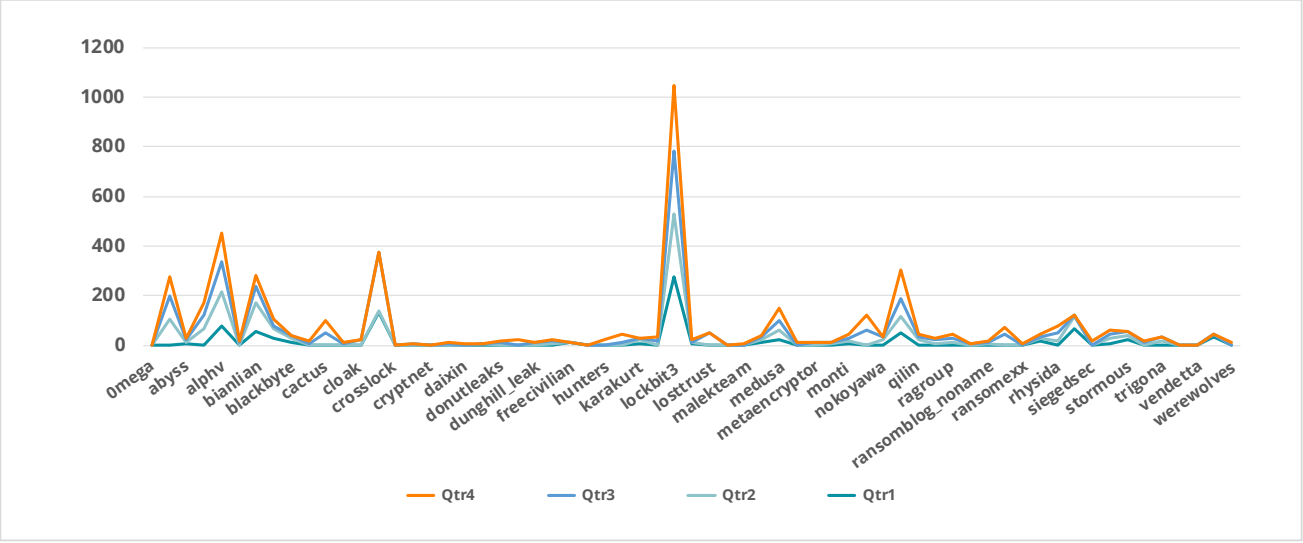
Ransomware Activity



All Threats by Volume, Q4 2023

The final quarter of 2023 (Oct 1st – Dec 31st) saw a total of 1,218 successful ransomware attacks against organizations. In Q3 we saw a total of 1,495 attacks, resulting in a 22% decrease quarter over quarter curiously.

This brings the total number of ransomware attacks in 2023 to 4,769, compared to 2,870 attacks in 2022. A 66% increase in attacks year over year. Lockbit come out in front again this quarter, with their final count at 263 attacks. Followed by AlphV and Play at 114 each, 8Base at 75, and NoEscape at 61.



Growth of Threat Actor Activity Quarter by Quarter 2023

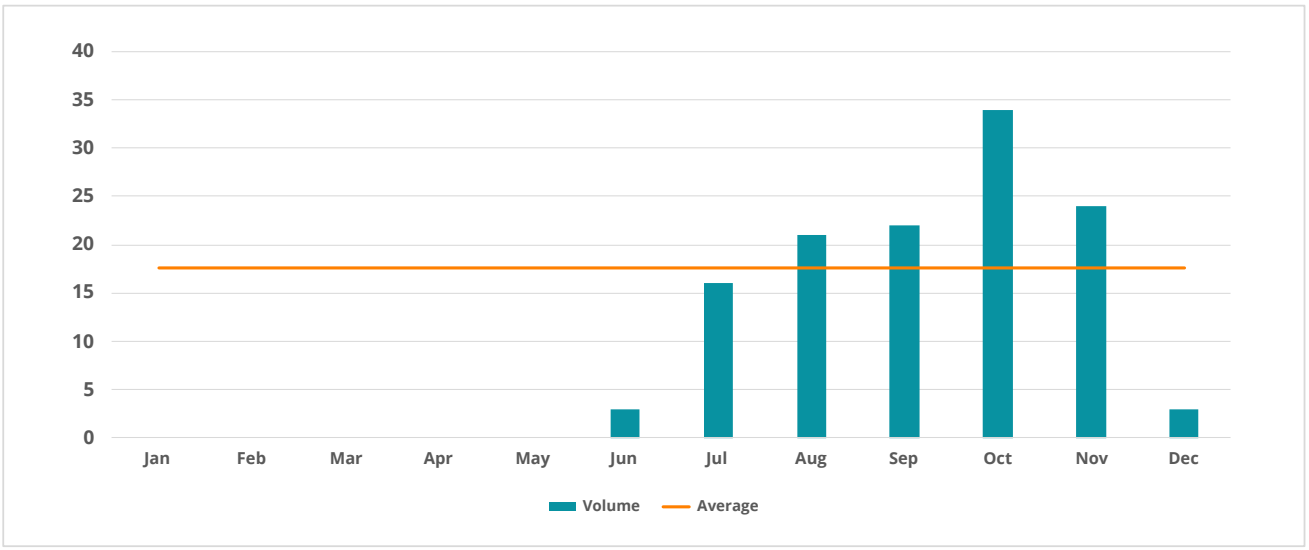
NoEscape

NoEscape Ransomware Group Dark Web Page

NoEscape are a relatively new group that we began monitoring back in June and have quickly made a name for themselves offering a RaaS (Ransomware-as-a-Service) model. They operate a shared profit model, with any ransom in excess of $3M USD running a 90/10 split for affiliates, or 80/20 for $1M USD payouts. Interestingly, NoEscape do not target groups in the CIS (Commonwealth of Independent States) in Eurasia, which may be indicative of where the group is based from.

NoEscape averaged 17.5 attacks per month this year (excl. non-activity months from January to May). NoEscape fall into the 'opportunistic' category of threats, targeting multiple organizations from various countries regardless of industry.

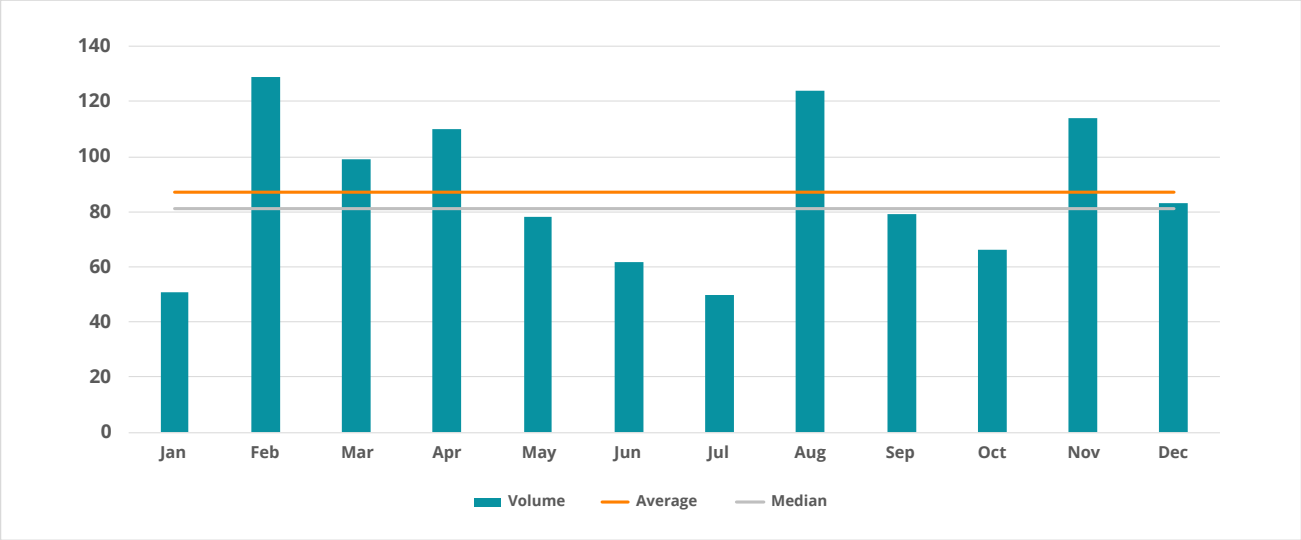
Map of CIS States



NoEscape Month-by-Month Ransomware Activity 2023

LockBit

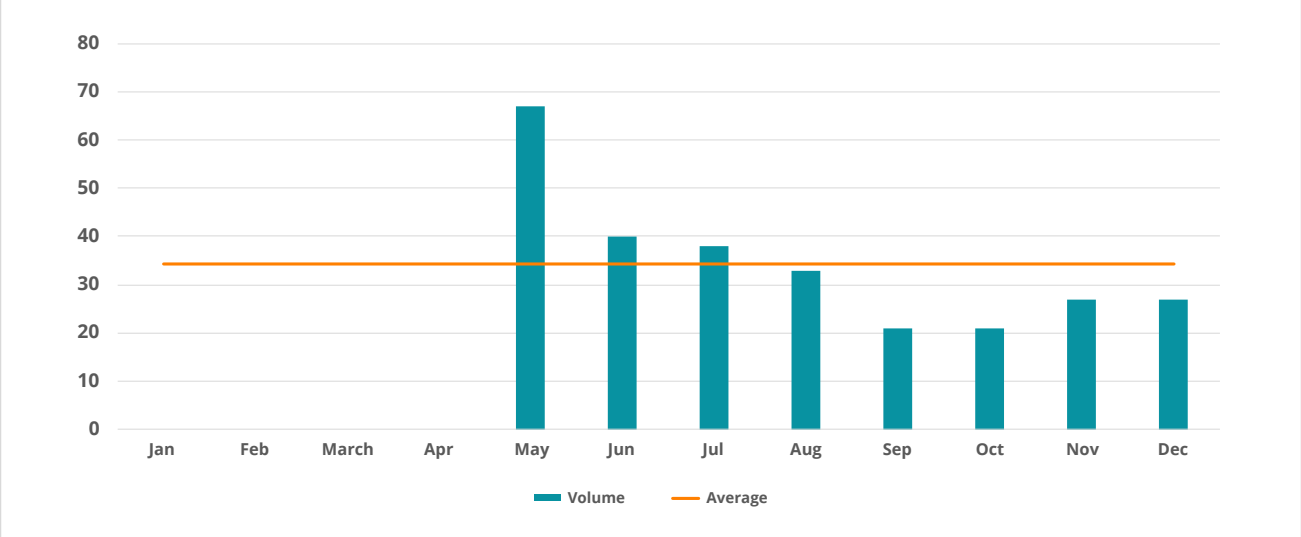
Lockbit, on average, completed 87 successful ransomware attacks each month with a median frequency of 81 attacks each month. Considering that Lockbit are highly opportunistic, utilizing initial access brokers to purchase access to systems, and target software vulnerabilities rather than specific industries directly; we can easily see why they have consistently been the most prolific ransomware group in 2023.



Lockbit Month-by-Month Ransomware Activity 2023

8Base

Earlier this year in Q2 we identified 8Base as an up-and-coming threat and added them to our watchlist. They have consistently appeared near the top of our tracking efforts since. 8base are also opportunistic and make use of all chances to exploit that comes across their path.



8Base Month-by-Month Ransomware Activity 2023

Looking Ahead into 2024

A common theme across the major incidents of this year is an assault on the supply chain, affecting customers downstream. These types of attacks are proving to be more and more lucrative for threat actors, as one successful compromise can grant them access to dozens or even hundreds of customer environments.

These types of proxy attacks aren't going away in 2024. CISOs should be mindful of who has access to their network and ensure that their vendor's security posture is to an acceptable standard that aligns with internal efforts being made to reduce the likelihood of falling victim to such attacks. Focus on NAC, tooling, and ensure that devices joining the network match said standard. Work with your security partners to perform risk assessment and make a note of the tooling they use to help reduce the attack surface and improve your posture.

CISOs should also make endeavors to update and maintain accurate inventory and SBOM within their environment. Shepherding the technologies that are active in your network will help security teams to identify abnormal activity (know normal), as well as provide you with the means to filter your intelligence to just the items that affect your teams, coordinating patch management, and needed architectural changes.

Initial Access teams continue to exploit unpatched systems, and most groups today have outsourced this part of their operation to dedicated teams so they can focus on post-breach coordination, exfiltration, and extortion. However, the teams that perform initial access now have a market for their efforts and will continue to exploit vulnerable systems and people. SBOM comes into focus here as well. Knowledge of what is your network combined with knowledge of who is exploiting those technologies can drive your security roadmap throughout the year.

Threat Actors with funding from interested parties will often make use of Ransomware as a Service, utilizing double-extortion tactics to ensure that data is exfiltrated out of the network. The goal here is often to increase the payments received from the victim organization. An ulterior motive may not immediately be obvious, in that the backing party will want to access to this data specifically – often leading to intellectual theft, stealing of secrets, and access to other sensitive information.

About CyberMaxx

CyberMaxx, LLC, founded in 2002, is a tech-enabled cybersecurity service provider headquartered in New York, NY. Through a comprehensive set of services CyberMaxx empowers customers to Assess, Monitor, and Manage cyber risk and stay ahead of emerging threats. CyberMaxx expanded its capabilities through the 2022 acquisition of CipherTechs, an international cybersecurity company providing a complete cybersecurity portfolio across MDR Services, Offensive Security, Governance, Risk & Compliance, DFIR, and 3rd-party security product sourcing.

CyberMaxx's managed detection and response solution (MAXX MDR) is designed to be scalable for clients of all sizes, providing protection and improving the organization's security posture, ultimately giving customers peace of mind that their systems and data are secure.

Learn More, Today!

To learn more about CyberMaxx's solutions please visit, CYBERMAXX.COM to get started.