CyberMaxx

Quarterly Ransomware Report Q2 2023

Published by CyberMaxx

Q2 2023 Quarterly Statement

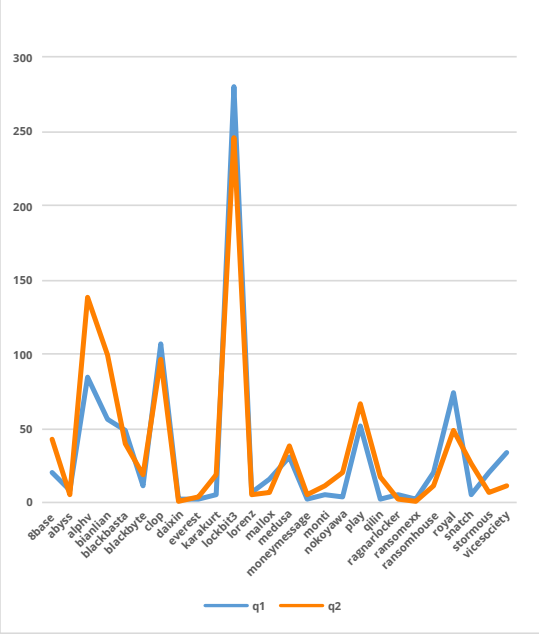
Executive Summary

While most Ransomware groups saw minor increases, AlphV, 8Base, BianLian, Karakurt, Nokoyawa, Play, Qilin, and Snatch showed significant growth. A noteworthy development is the emergence of 8Base, a new group that has rapidly gained prominence throughout Q2 2023. With a total volume of attacks in June rivalling Lockbit, 8Base is quickly becoming a notable name in the ransomware landscape.

Ransomware attacks have shown a significant increase in the second quarter of 2023, with a 26% overall rise compared to the previous quarter, with Lockbit leading the pack.

Another significant event in Q2 2023 was the exploitation of a vulnerability in Progress Software's MOVEit file transfer service, impacting over 200 organizations. The Cl0p ransomware group claimed responsibility for the widespread exploitation, resulting in a large volume of successful attacks. Exploitation of unpatched vulnerable devices remains a common trend, leading to various malicious activities within compromised systems. Further downstream organizations and appliances were also targeted post exploitation by the Cl0p group. Cl0p is still working through their backlog of victims. Once they confirm the attack on their release page, we include the attack in this report. As a result, the total number of confirmed attacks for Cl0p this quarter is less than they have officially confirmed by releasing the affected organizations name.

Looking ahead, it is expected that 8Base will continue to be a prominent threat actor in the upcoming quarter. However, they currently rely on established techniques used by other groups and do not exhibit novel tactics. Therefore, it is crucial to prioritize patching vulnerable devices to mitigate the risk posed by unpatched services and infrastructure.



2023 Q1 vs 2023 Q2 ransomware activity by volume and group

Ransomware Attacks are Up this Quarter

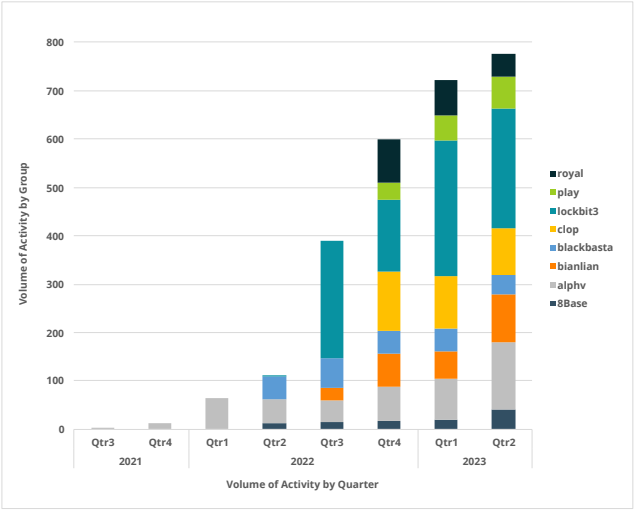
The second quarter of 2023 (April 1 – June 30) revealed a 26% overall increase in ransomware attacks; up from 909 in Q1 to 1147 in Q2. Lockbit is still leading the way with attacks, while most of the other ransomware groups have also increased their efforts.

Lockbit remains the most prolific group again this quarter, with 246 attacks attributed to them, or 21.4% of all ransomware attacks, down from 278 in Q1 2023. Several other groups have shown steady numbers throughout both Q1 and Q2 2023, such as Lorenz, and BlackBasta.

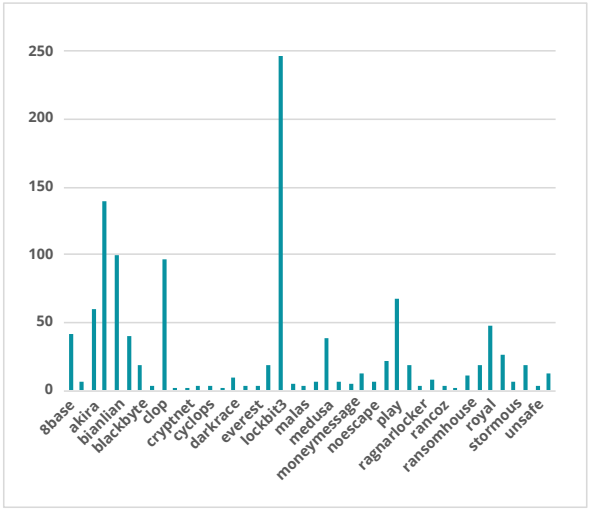
Overall, activity is largely evenly distributed across the board. Most ransomware groups are showing a minor increase in activity, with a small number showing a larger increase in their efforts across AlphV, 8Base, BianLian, Karakurt, Nokoyawa, Play, Qilin and Snatch. This is a visualization of this activity trend.

Ransomware attacks do not happen in isolation. They require several stages to be completed from initial access, lateral movement, escalation of privileges though to completion of their objective. A successful attack usually occurs if there is a gap in one or several layers of an environment's security stack.

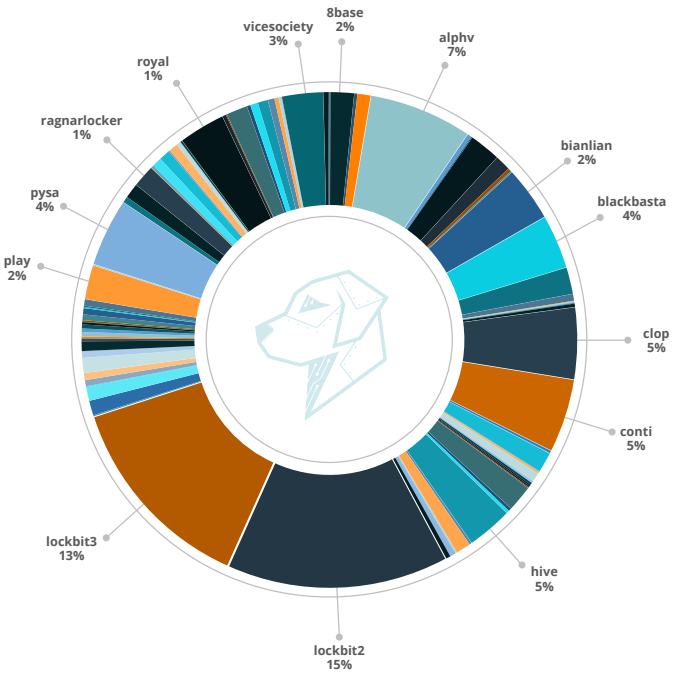
Based on the tactics, techniques and procedures of the Threat Actors with increased activity this quarter, the large increase observed is likely due to a mix of unpatched, vulnerable services being exploited, as well as a continuation of social engineering attacks against unsuspecting users. Both of these beachhead tactics are a common trend we have witnessed during incident response engagements.



Total volume of activity by quarter of several active and growing threat groups



Distribution of all threat actors by volume for Q2 2023

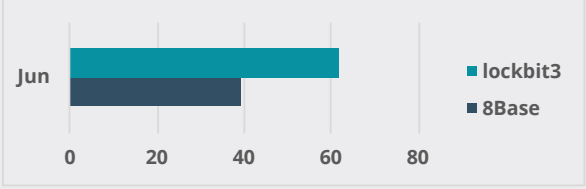


Total Ransomware distribution by percentage for Q2 2023

The Rise of 8Base

8Base is a new group that we began tracking last quarter after we found they had begun gaining a larger presence, which only continued to increase throughout Q2 2023.

8Base, who are self-described as "honest and simple pentesters", began ramping up operations in May 2023, and brought their total volume of attacks up to rival LockBit as of June 2023. Total Lockbit volume was observed at 62 and 8Base at 39 successful attacks.

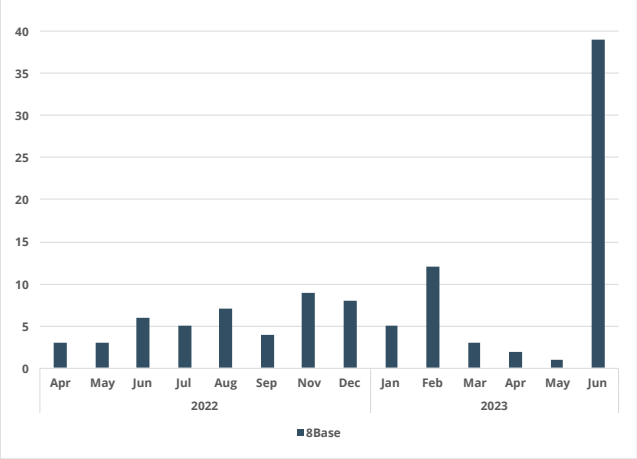


What We Know: 8Base and RansomHouse

Our research shows that there have been significant similarities between 8Base and RansomHouse. Based on the ransomware notes and leaked sites of both, verbiage and languages are nearly identical. It is undetermined, but there is a probability that 8Base could be an affiliate or copycat of RansomHouse.

In addition, there has been a sample recovered for 8Base where Phobos 2.9.1 was loaded with SmokeLoader for initial access. Phobos being available as a ransomware-as-a-service, it comes to no surprise of its use as threat actors can customize parts of it to their needs, which was seen in the sample from 8Base by changing the appendage to 8Base for their encrypted files.

The complete formatted appendage matched the same as Phobos as it included an ID section, email address, and the file extension. Also from the sample, 8Base was observed using SystemBC, a remote administration tool in use by several other groups to aid efforts with encryption and concealing their C2 infrastructure.



Distribution of activity for 8Base

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.

A screenshot taken from Cl0ps dark web page

MOVEit Vulnerability

This quarter a vulnerability in Progress Softwares MOVEit file transfer service impacted over 200 individual organizations. Our Threat Hunting team closely monitored the situation around exploitation of the MOVEit vulnerability and ensured that detections were in place to combat this, as well as hunting for new indicators as they became available.

The Cl0p ransomware group have taken credit for the mass exploitation of MOVEit across compromised systems, affecting other organizations further downstream. The volume of successful exploitation was so widespread in fact, that Cl0p stopped reaching out to users individually and advised that they go to their PR page for general instructions on how to proceed. The image was taken from their dark web release page.

Exploitation of unpatched vulnerable devices continues to be a common trend across both initial access, as well as post-intrusion leading to privilege escalation, persistence and lateral movement within a domain.

Future Expectations

We are expecting to see a continued upward trend from 8Base over the following quarter, remaining in the top groups for activity. They currently do not display any novel tactics that separate them from other groups at this time, and instead rely on tried and tested techniques in use by other threat actors.

Sample Sentinelone STAR Rule

```
(Url In Contains Anycase ("admlogs25.xyz", "serverlogs37.xyz", "dnm777.xyz", "admlog2.xyz",
"admhexlogs25.xyz", "wlaexfpxrs.org", "dexblog.xyz", "blogstat355.xyz", "blogstatserv25.xyz") AND
(UrlAction = "GET" OR UrlAction = "POST")) OR (FilePath StartsWithCIS "c:\$recycle.bin" AND FilePath
EndsWithCIS "8base") OR (FilePath EndsWith ".8base" OR FilePath EndsWith ".eightbase") OR Url ContainsCIS
"t.me/8base"
```

Key Takeaways

- 8Base is quickly becoming a prevalent name, competing with Lockbit in June and ranking at #2 for the month when measuring volume of successful attacks
- Prioritize patching your vulnerable devices to stay ahead of opportunistic attackers who continue to make use of unpatched services
- Ransomware attacks aren't slowing down, so keep good security hygiene and maintain best practices whenever possible

The second quarter of 2023 witnessed a significant increase of 26% in ransomware attacks, with Lockbit leading the way. While most ransomware groups experienced minor activity growth, certain groups, including AlphV, 8Base, BianLian, Karakurt, Nokoyawa, Play, Qilin, and Snatch, showed activity increases. Notably, the recent rise of 8Base as a major player has been observed, with their attack volume rivalling that of Lockbit over the month of June.

Research indicates similarities between 8Base and RansomHouse, suggesting a potential affiliation or copycat relationship. 8Base has been observed customizing Phobos 2.9.1 with SmokeLoader and utilizing SystemBC as a proxy and remote administration tool.

The MOVEit vulnerability impacted over 200 organizations, with Cl0p ransomware group claiming responsibility for its widespread exploitation. Exploiting unpatched vulnerable devices remains a prevalent trend, leading to various malicious activities.

Ransomware attacks aren't slowing down, so keep good security hygiene and maintain best practices whenever possible.

Looking Ahead

8Base is expected to maintain its prominence, although it currently relies on established techniques that can be protected against. It is crucial for organizations to prioritize patching vulnerable devices and implementing robust security measures to mitigate risks posed by the unpatched software such as the rapid and widespread exploitation of the MOVEit vulnerability, alongside the ongoing increase in ransomware attacks exploiting these unpatched services.

The CyberMaxx Quarterly Ransomware Report is compiled and published by Connor Jackson, Security Research Manager at CyberMaxx, with a background in forensics, reverse engineering, and threat-hunting.

Quarterly Ransomware Report: Our Mission

The CyberMaxx team of cyber researchers conduct routine threat research independent of client engagements. The purpose of our research is to help foster collective intelligence among the cybersecurity community. We believe that by sharing the intelligence available to us with the broader cybersecurity community, organizations can more effectively stay ahead of the ever-evolving threats we all face. These threats negatively impact the operations of corporations and government entities as well as the lives of innocent consumers.

While conducting their research, the team discovers and analyzes ongoing ransomware attacks occurring in the wild. The intelligence gathered from these efforts is then reported on quarterly, adding further insights into previously reported activity. The Q1 report can be downloaded HERE on our website.

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.