



Q3 2023 Quarterly Statement

Executive Summary

The third quarter of 2023 (July 1st – September 30th) has seen several notable events, with large conglomerates being targeted by threat actors, to new malware strains having a lot of success with a recent change to their model.

One of these notable events that we observed was a major ransomware attack on the MGM group. The attack curiously has been claimed by two separate threat actors, AlphV and Scattered Spider – who both have made claims here. It is currently unclear whether they were working together at various stages of the operation or not at this time.

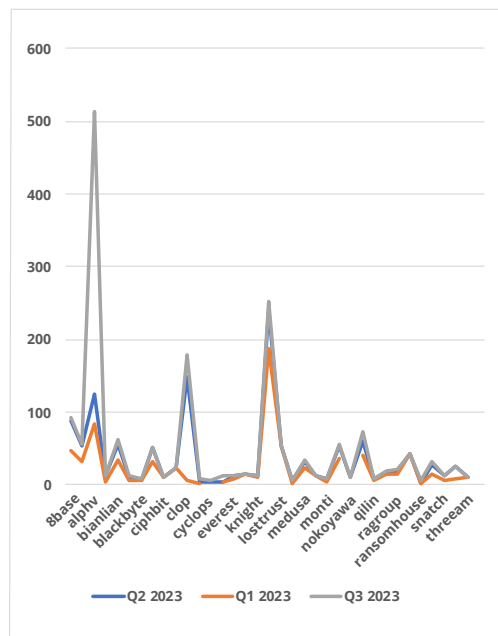
Other notable groups include Cl0p, who still appear to be working through the backlog from exploitation of the Movelt Vulnerability earlier this year, and Lockbit who are a regular contender in terms of volume in our tracking efforts. 8Base continues to have a large impact based on the frequency and volume of their attacks this quarter.

An existing malware strain 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.

Our tracking of high impact groups shows 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.



The third quarter of 2023 has seen a staggering increase of 59% over Q2, with the AlphV Threat Group making up 28% of that total figure.



Comparison: Q1 vs Q2 vs Q3

Ransomware Activity

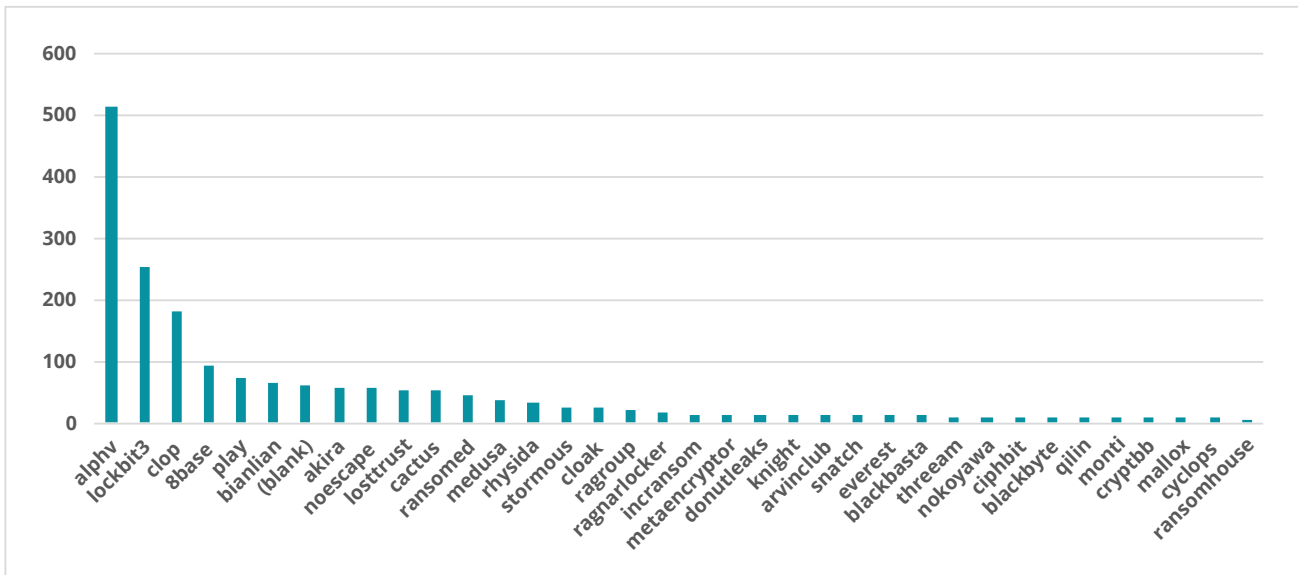
Attacks Have Continued to Increase This Quarter

The third quarter of 2023 (July 1 to September 30) has seen a staggering increase of 59% over Q2, with the AlphV Threat Group making up 28% of that total figure. AlphV have contributed 512 successful ransomware attacks to the total volume this quarter, making up 28% of the overall figure. Including other groups the total number is 1826 successful attacks.

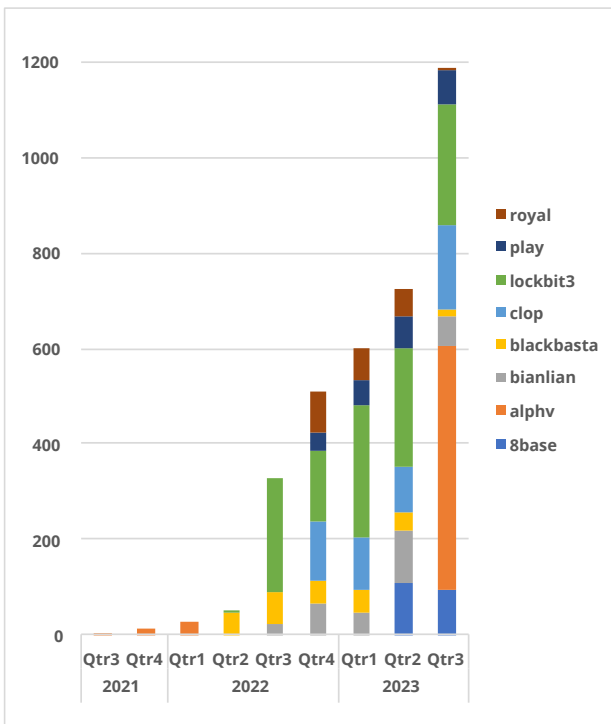
Looking back on 2023 so far, Q1 had 909 total attacks and Q2 had 1147. We are seeing a steady rise of attacks quarter-on-quarter, which doesn't appear to be going away any time soon.

Q3 showed an increase in activity across almost all groups, with a handful maintaining the same volume as last quarter. No groups have shown a decline in activity in Q3 2023, with groups such as AlphV having a dramatic increase of over 400%.

The top five groups ranked by volume are Alphv, Lockbit, Cl0p, 8base, and Play.

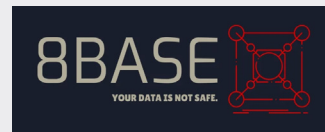


Distribution of threat actor activity by volume for Q3 2023



High-Impact Group Tracking for 2021-2023

The Rise of 8Base



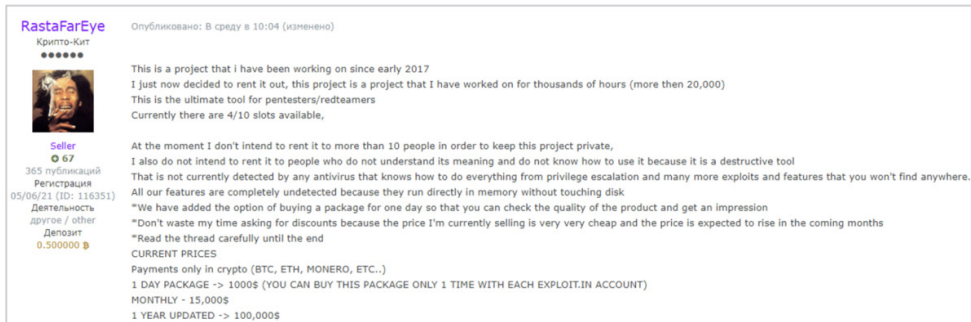
We previously predicted that 8Base would continue to have a large impact on the industry. This has been proven to be correct with the following volume of successful attacks having been observed:

- Q2: 107
- Q3: 92

While they haven't had more successful attacks than the previous quarter, they still have successfully completed a significant volume of attacks. 8Base are currently ranked as #4 in volume of activity for Q3 2023.

DarkGate Malware

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.



The screenshot shows a forum post by user RastaFarEye. The post title is "Крипто-Кит" (Crypto-Kit). The post content includes a description of the malware, its features, and pricing. The pricing is listed as follows:

Package	Price
1 DAY PACKAGE ->	1000\$ (YOU CAN BUY THIS PACKAGE ONLY 1 TIME WITH EACH EXPLOIT.IN ACCOUNT)
MONTHLY ->	15,000\$
1 YEAR UPDATED ->	100,000\$

Original Listing of DarkGate by Developer, RastaFarEye

A full analysis of the malware strain can be found at this link: <https://www.cybermaxx.com/resources/darkgate-malware-initial-loaders-and-how-to-mitigate-issues/>

Sentinelone and CrowdStrike Rules That Can Be Used to Detect Darkgate

SentinelOne Rule

```
(CmdLine ContainsCIS "/c mkdir" AND CmdLine Contains Anycase "copy" AND CmdLine ContainsCIS "autoit3" )
OR (CmdLine ContainsCIS "user-agent: curl" AND EndpointOS = "windows") OR (CmdLine ContainsCIS "/k curl"
OR CmdLine ContainsCIS "curl -# -o") OR CmdLine ContainsCIS "c\"u\"r\"l"
```

CrowdStrike Rules

```
CommandLine IN(".*curl*", ".*c\"ur\"l*", ".*c\"u\"r\"l*", ".*c\"u\"r\"l*") AND CommandLine
IN(".*autoit3*", ".*autolt3*") AND CommandLine = ".*http*"
```

```
(event_simpleName=ProcessRollup2 OR event_simpleName=ScriptControlDetectInfo) AND (FileName
IN("cmd.exe", "powershell.exe", "pwsh.exe", "wscript.exe", "cscript.exe", "regsvr32.exe", "rundll32.exe", "msiexec.exe", "cerutil.exe", "mshta.exe", "csc.exe", "bitsadmin.exe", "msbuild.exe", "wmic.exe", "windbg.exe", "cmstp.exe", "cdb.exe") OR ParentBaseFileName
IN("cmd.exe", "powershell.exe", "pwsh.exe", "wscript.exe", "cscript.exe", "regsvr32.exe", "rundll32.exe", "msiexec.exe", "cerutil.exe", "mshta.exe", "csc.exe", "bitsadmin.exe", "msbuild.exe", "wmic.exe", "windbg.exe", "cmstp.exe", "cdb.exe")) AND ((CommandLine = ".*curl*" AND CommandLine = ".*autoit*" AND CommandLine = ".*http*"))
```

```
CommandLine = ".*cmd.exe*" AND CommandLine = ".*curl*" AND CommandLine = ".*autoit*" AND CommandLine = ".*http*"
```

Key Takeaways

- Supply Chain attacks are continuing to be a lucrative vector for attackers, and is being used to target large organizations
- Malware as a Service (Maas) is continuing to rise in popularity, DarkGate is a versatile loader that should be monitored for alongside strains such as Emotet, QakBot, Redline and several others

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 Q2 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.

