Hello, everyone.

As you may be aware, all Seal services, including the website, wiki, bug board, IRC, and all other services went offline for a period of > 6 hours on Sunday, May 2nd, 2021.

Due to the length of time the services were offline, we thought that it would be best that we reach out to you regarding what happened, what went wrong, and what we're doing in response. This is in line with, but not explicitly required by, our Terms of Service, Privacy Policies, and other applicable policies. Regardless, in the spirit of open communication and transparency, we've prepared this report.

First and foremost, I want to say that we do not have any reason to believe that any accounts or user data was accessed, nor was this a directed incident against the Seals. At no time did an unauthorized user access our systems.

So, let's jump into it.

What Happened?

On 2021-05-02 at around 5:33 GMT, the Seal main web server experienced a "rapid unscheduled disassembly" - or more properly, the Linux server we use to host stopped responding to all server input. This was brought on by the Apache web server software we use running out of accessible memory, and as such the server killed all nonessential processes in order to keep itself alive (OOM-KILL, OOM-REAPER). Unfortunately, this process made the server inaccessible to us. In short order, the IRC services (ChanServ, etc) lost their connection to the MySQL server we use for our data storage, as the server it was hosted on was no longer responding to anyone. This caused an unknown issue with Anope that resulted in not only the IRC server but also the main server entering a fail state. Normally, the systems are independent of each other (where if one server goes down, the others can survive), however for some reason this time a clean disconnect did not occur.

This situation was not noticed for around two hours, as the symptoms of the IRC server being offline presented themselves. Unfortunately, the CyberSeal who noticed this situation did not have the access to remedy the issue. All three of the users who have the ability to bring some or all of the services back online in the event of a catastrophic failure were either asleep, offline, or unable to respond. It was not until around 6 hours after the start of the incident that the proper staff could be summoned and assembled to solve the issue. Two of the "key three" started diagnosis work at 1430 GMT, and all three of the "Key Three" were assembled by 1514 GMT. After resolution work started on the server by all three of the key staff members, the issues were resolved and service functionality was restored within 5 minutes, with full service functionality restored at 1518 GMT.

What Went Wrong?

After being informed of the incident, we began working to investigate the source of the issue. We informed the Staff core of the incident, and a few preliminary indicators made us think this might be a direct attack on Seal services or an attempt to access our systems. Under that assumption, we began tracking down all access, kernel, system, and web logs we had access to, as well as Amazon Web Services (our host) logs to figure out what the source of the issue was. Truth be told, it sounds like Microsoft accidentally DoS'd us. BingBOT, one of Microsoft's search crawlers, repeatedly tried to access a file on our web server, which did not exist. Something on the site had given the impression to the search crawler that we used WordPress, and so looked in several different (also non-existent) locations at the same time. Our logs show over 262 access attempts in short order from a short range of IP addresses all belonging to the same owner - Microsoft. (Damn you, Bill!) While at first this appeared to be the result of a targeted attack on the WordPress system, further investigation eliminated that as a reasonable explanation.

In addition, as part of having a SSH server running out in the wild, our servers are frequently pinged by random bots attempting to break in. These range from simple dictionary attacks, where various usernames and passwords are tried, to complex attempts to guess the security keys used for master accounts. We monitor these closely, however we have not seen any of these even remotely come close to succeeding.

Usually, our server can handle this load no problem. However, a perfect storm of unlikely unfortunate events meant that the system did not have enough free memory to process all those requests at the same time, resulting in excessively high memory usage, and a crash. We are working to prevent such an instance from happening again.

What are we doing to fix this?

After the event and immediate clearing of the event, we began a self-audit and checked exactly what went wrong, what could have been done better, and how to improve our systems. While we are not done with this process, we have made some preliminary changes to our procedures, systems, and policies to help mitigate this situation.

1. We have enabled a new bot firewall for our web traffic on the Seal domains.
2. We have added a new sitemap and site instructions for Web Crawlers to limit their impact on the site.
3. We have run a few optimization passes, including upgrading our PHP version, on the Seal site to reduce memory usage and increase speed.
4. We've added new monitoring systems to alert our Techs on issues more reliably.
5. In the event our main servers are unreachable, we have set up an automatic process in an attempt to restart them.

6. We’ve enabled a stricter logging and banning system on unsuccessful attempts to log in to the Seal server backend.

While these solutions do not solve all of the identified issues, they are the first step we have. Upcoming HalpyBOT and Site updates will focus on access, reliability, and stability, and we are working on how to best cover our time zones among the “key three” cybers, and deal with other issues as we discover them.

Thank you for reading, and we apologize for the disruption in services caused by these issues. I would like to especially thank our CyberSeals for their quick attention and resolution of the issue, once everyone was assembled, and their eyes in sorting through the logs. (You would not believe how many logs our servers generate… CVS receipts put to shame).

As always, we are more than happy to answer any questions you may have. Please feel free to DM us on Discord or email us at cyberseals@hullseals.space.

Fly safely, CMDRs.

Rixxan
The Hull Seals