Everything You Need to Know about the Notorious Zeus Gameover Malware

By Morten Kjaersgaard

Published: 2021-08-27 · Archived: 2026-04-05 13:58:56 UTC

When you read the headline you may actually think that this is *game over* for the Zeus malware, but in fact, we are talking about the **Zeus Gameover P2P** variant. This new variant, where Heimdal was recently involved in a global takedown with FBI and Europol, is the latest evolvement in a piece of highly advanced malware.

To give you an overview of the problem, we must understand what **Zeus P2P does, why it spreads and how widespread it is.**

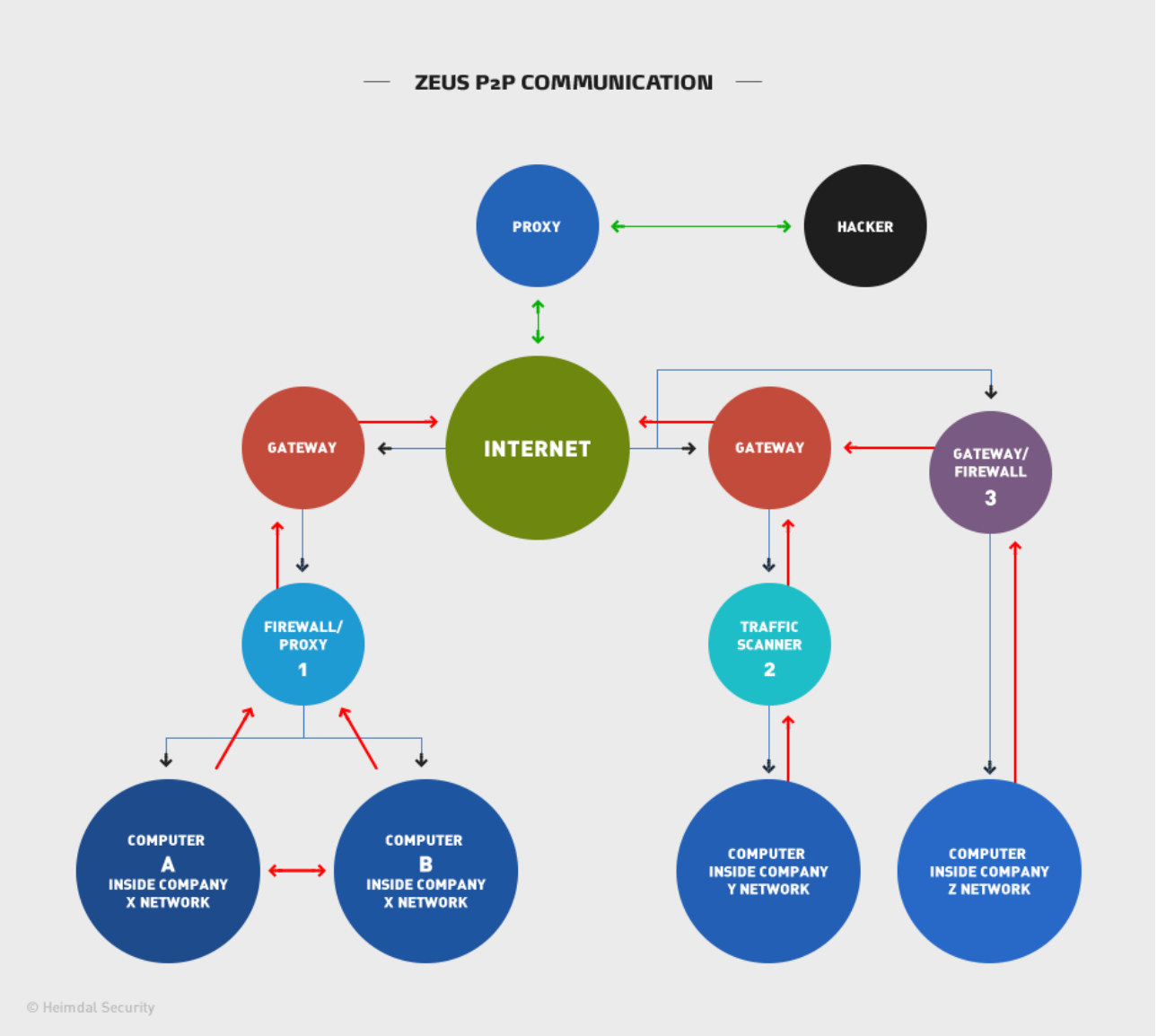
How does Zeus Gameover work?

First of all, this variant of the malware poses a **real problem**, because it *constantly looks for data* on your network or PC, which is identified as valuable, either via identification commands or via prefixed algorithms.

Typically, a Zeus infection looks for ***personal data***, ***credit card information***, ***customer data*** or ***secret corporate information.***

After Zeus P2P finds what it is looking for, it will be able to instantly send that information to other peers in its network, **anywhere in the world**. This means that data from your internal network can be shifted out of the network instantly to another computer, which is also in the Zeus P2P network. *This computer can be located anywhere.*

The illustration below shows a simple overview of Zeus P2P communication.



The blue lines on the illustration indicate incoming traffic and the red lines indicate outgoing traffic.

How to secure your company from Zeus GameOver?

If your company uses a **Firewall** or **Proxy**, as indicated in the diagram note 1, you have a *relatively* good protection if your proxy is updated and it knows what to look for. Most likely though, **it isn't**, because Zeus Gameover communicates with other companies and IP addresses that you probably wouldn't want to block because it would prohibit your employees from working.

Blocking at proxy level would mean **enforcing** organization-wide **limitations**. This will result in less productivity for your entire organization, not just the infected computer. Now you might be thinking, "*how much would we be blocking?*".

Well, honestly, a LOT! Thousands of corporations out there are infected with Zeus P2P and as many as **1.2 million computers were infected prior to the takedown of Zeus.**

That number is lower now, but they can easily pick up if the infrastructure is rebuilt and still many computers are infected, so you would be blocking widely.

The same problem arises with **traffic scanners** as per note 2, which work at a corporate level, as they would block entire IP ranges or DNS ranges.

If you are a smaller company just using an **antivirus** solution, **gateway** or **firewall**, as per note 3, you are simply ***highly exposed*** to the Zeus P2P dangers, because it will pass straight through your security measures. See what the difference between antivirus and antimalware is and how they should complement each other.

In relation to note 1 and 2, although not related to Zeus Gameover, I would like to give you an example of a similar problem that antivirus makers are facing, just to give you a picture you could potentially relate to.

Some antivirus manufacturers have a similar problem to corporate-wide blocking, where they block entire websites, instead of just the malicious content that their scanner found on a given website. These "false positives" result in your company being blocked from using services on legitimate websites, which could be anything from government to private enterprises.

[Tweet "Do you know how the most vicious financial malware in history worked? Our CEO explains it:"]

So why is it so difficult to protect yourself from Zeus P2P Gameover?

Well, first of all it is a **highly persistent threat**, which infects networks with low detection rates, due to its **polymorphic** nature.

Secondly, once infected it is hard to remove the infection from a client, due to the new Gameover version, which contains a **Necurs rootkit**. This often means that the easiest way of getting rid of the problem is to wipe the infected client. However, chances are that it will easily get infected again.

Thirdly, once Zeus is inside it will *easily* communicate with other peers or look for new ones if the ones on its default list are unreachable. If that also fails, Zeus will turn to its DGA (Domain generation algorithm) to find peers.

Why isn't it possible to block Zeus traffic then?

Well, as described above, if you block at a corporate level, then you will block all domains or IP addresses, which are Zeus infected. First of all, obtaining data about who is infected is more than difficult and requires a security solution with massive intelligence. Secondly, it's not viable, because you will be blocking so much that you will prohibit your organization from working efficiently.

How can you best relate this problem to the real world?

Well, *imagine you live in New York City.* You and your family (your PC) live at 5th Avenue and your friend (wsj.com) lives on Wall Street. You know that someone on your friend's street is sick with a virus, so you prohibit your family from visiting, by blocking the entrance to Wall Street. Then naturally you can't get in to visit, but your daughter needs something from your friend, so the only way to make that happen is to open the roadblock.

Jumping back to cyberspace, what you could do is to use client software to block the infection. This way you can both prohibit your computer from spreading the infection, and at the same time prohibit your computer from

sending and receiving information to and from other peers and the controlling servers.

[Tweet “The Zeus Gameover malware caused millions in financial damage. Here’s how it did it:”]

How Heimdal can help to protect you from Zeus Gameover?

One way to do this is using **Heimdal Threat Prevention**, as it has the intelligence capability to block this. It works by prohibiting an infected computer from talking to DGA servers or from talking to known infected websites or addresses. This means that you can even install Heimdal on an infected computer and it would **block the data trying to be sent from your computer.**

Heimdal also offers infection detection by spotting the communication attempts.

Why can’t you just use your antivirus solution? Well, having a history in the antivirus industry at BullGuard as CCO, I might be a little biased in what antivirus I would favor. But generally speaking, antivirus solutions focus mainly on file behavior or behavior on the computer. Some also depend on other heuristic algorithms or behavioral engines.

With morphing viruses such as Zeus that means a low detection rate, because **the signature and MD5 hash changes all the time**. This is also why Zeus is effectively able to spread.

Does this mean that you should just scrap your antivirus solution? **No, absolutely not**, but it does mean that you need **multiple layers of protection** on the client.

Heimdal®

Antivirus is no longer enough to keep an organization’s systems secure.

Heimdal® DNS Security Solution

Is our next gen proactive DNS-Layer security that stops unknown threats before they reach your endpoints.

- Machine learning powered scans for all incoming online traffic;
- Stops data breaches before sensitive info can be exposed to the outside;
- Advanced DNS, HTTP and HTTPS filtering for all your endpoints;
- Protection against data leakage, APTs, ransomware and exploits;

Conclusion

Reviewing the extent of the Zeus Gameover P2P problem, the latest numbers in our database would estimate that as many as **1.2 million computers worldwide were infected** up until the takedown operation. The worst fears are that this number could easily recover if the infrastructure is restored.

Zeus P2P tried to Gameover the antivirus industry with its latest version and the struggle is still ongoing.

Morten Kjaersgaard is the Founder and Chairman of Heimdal®, a global leader in AI-powered cybersecurity. Under his leadership, Heimdal has grown from a startup in Copenhagen to a trusted security partner for over 16,000 organizations and more than 2,000 MSPs worldwide, defending against 260+ million cyber threats annually. With a sharp focus on unifying cybersecurity operations, Morten is recognized for his ability to align technical innovation with strategic business outcomes. His insights have shaped how organizations and partners alike approach risk reduction, compliance, and security maturity in an increasingly complex digital world. A respected voice in the industry, Morten frequently shares his expertise at international events and through media commentary—championing a more proactive, collaborative, and scalable model for cybersecurity success.
