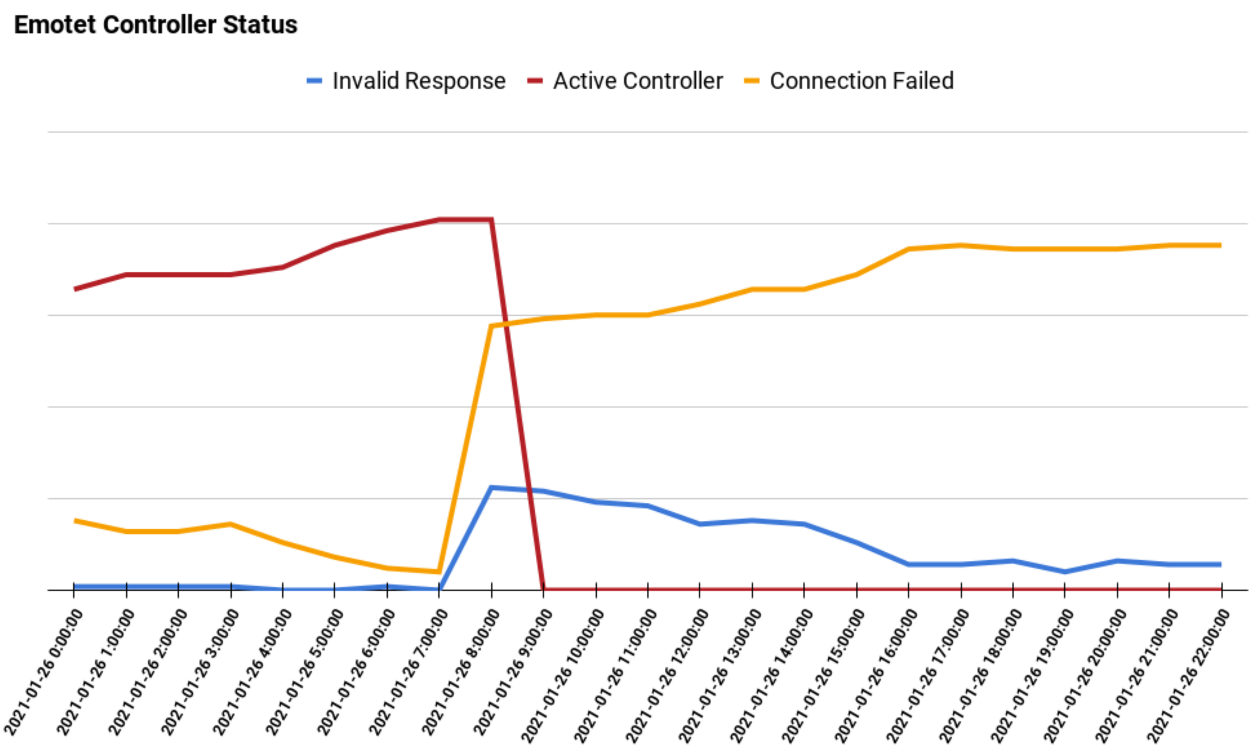
Taking Down Emotet

team-cymru.com/blog/2021/01/27/taking-down-emotet/

James Shank View all posts by James Shank January 27, 2021



On Tuesday, January 26, 2021, the number of available controllers talking like Emotet Tier 1 controllers dropped to zero.

Team Cymru's monitoring confirmed that they dropped from over 100 to zero in a really short timeframe. That's interesting.

Helping to make that happen? That's fun.

Let's talk about the fun!

A Call and a Request

A friend of mine phoned me a couple weeks prior. "Hey man, how are you? I've got something Team Cymru might be able to make happen." "Doing well! What's on your mind?"…

It's no secret that law enforcement agencies have been tracking Emotet. Any threat that generates over a certain threshold of losses per year draws attention. Emotet has "cost [state, local, tribal, and territorial] governments up to $1 million per incident to remediate”. When the U.S. Department of Homeland Security puts that price tag on a threat, law enforcement is already taking note.

“Here’s what we want to do…”

Coordinated Operations

Law enforcement authorities in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine were getting close to executing a plan to take down Emotet. They were working their processes, coordinating a time to award some handcuffs. The teams also coordinated taking over parts of the Emotet infrastructure. Where possible, these systems would change hands and would no longer harm victims.

While these and the other collaborating law enforcement agencies have a long reach, they can’t reach everything. In some countries, Emotet’s activities aren’t illegal — unless that country’s citizens are victims. International law enforcement collaboration varies between countries. Add to this that some hosting providers may have ties to criminal enterprise. Serving papers on upcoming activity may become a signal that allows the actors to get away.

This creates a problem. Taking over only part of a botnet is not ideal, and doing so may allow the actors to reclaim control. How can systems that legal process can’t reach, shouldn’t reach, or won’t reach on time be in scope?

The Untouchables

“Can we get networks to block the servers that aren’t taken over?”

Make no mistake, large networks exist for one primary reason: move packets. This is their job, their raison d’être. When you ask networks to block packets, you’re asking them to put their neck on the line. The concerns are quite reasonable: reliability, liability, and collateral damage are at the top.

“We may have a shot. Let’s try. We may get 65% to help out.”

Getting these untouchable systems blocked is important to the goal. Emotet actors break into systems or buy access to systems already compromised. If an infected client connects to an actor controlled system, they will incur further harm. If they reach a system controlled by law enforcement after the take over, they won’t be harmed.

Emotet Configs and Controller Selection

Emotet has three different botnets, Epoch 1, Epoch 2, and Epoch 3. These three botnets have different victim-facing controllers. When a client gets the initial binary, that binary contains a list of up to 100 controllers from one of these three groups.

The malware will attempt to connect to one of the controllers in its config data. If this succeeds, great, but if it fails, it will try another controller on the list. It will keep doing this until it either connects to a controller or exhausts the list.

“We want the clients to connect to the seized servers.”

Given the selection process, and that the reach of law enforcement is only so far, we need to block some servers. Blocking servers will cause the malware to try other servers in the config. The first server to work, we hope, will be one of the seized servers.

Team Cymru has our own sources for Emotet controller data. We combined our sources with the excellent work of Cryptolaemus, a community effort to fight Emotet. We then validated these data points with Team Cymru’s processing. After aggregating these results with one other data source, we made the kill list available to network operators.

The Network Operator Responses

Of the network operators invited to the organizing calls, only one declined. The reason was quite reasonable: without legal paperwork, their network will not act. This is a respectable position; when compelled to act, networks are not liable.

For the networks that joined the calls, they all helped in this effort except one. That network had a change freeze due to lockdowns related to COVID-19. Because lockdowns may prevent their staff from gaining physical access to their equipment, they could not risk changes that were unnecessary. This Emotet take down effort, while good and the desire to help was there, was not necessary.

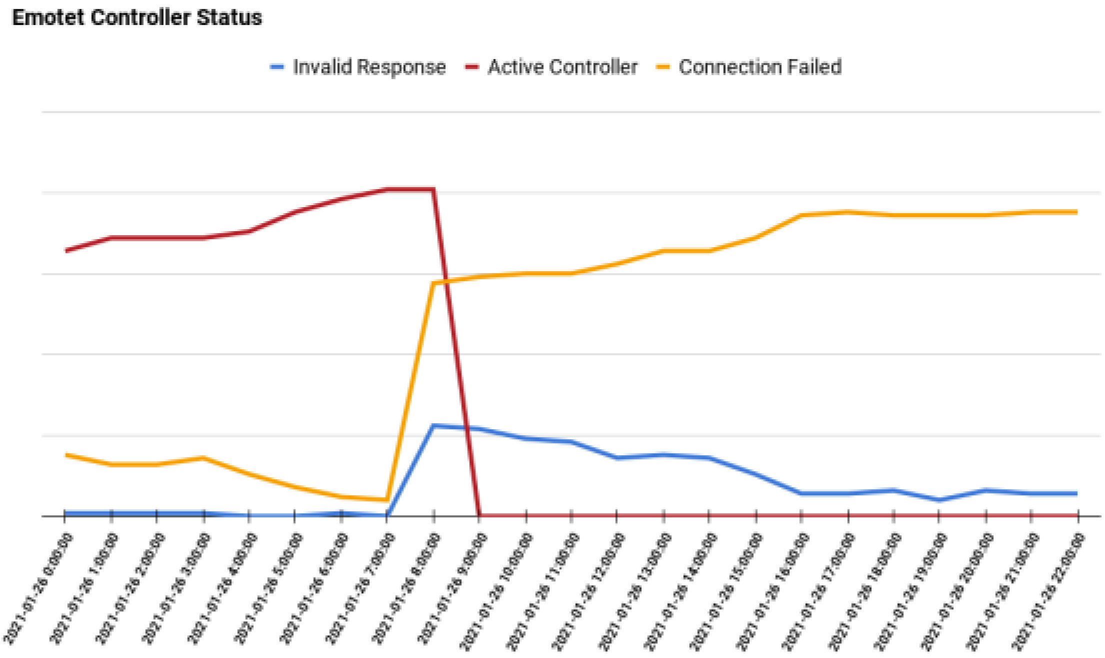
This participation rate was well above my prediction of 65%. Those that know me may say I’m a shade pessimistic. The results speak for themselves.

The Results

“We’re not seeing any active Emotet Tier 1 C2s now.”

Team Cymru has several systems that track threats. One of our more advanced bot tracking systems is our Botnet Analysis and Reporting Service (BARS). This system takes controller data from several inputs and maintains up-to-date information on the controller status. We’re not new to this game, and we know it is common for botnet operators to feed invalid configuration data. They do this to trip up researchers that do not have validation processes in place.

For Emotet, we connect to the controllers and check for expected responses. We connect out from several network exits around the world. This morning, our BARS service saw a pronounced change.



Tier 1 controllers drop from 100 to zero.

What this shows is the initial Emotet takeover was a profound success. The “Invalid Response” shown above are the seized servers. Team Cymru’s validation rules show that these servers did not match expected responses. The blocking of the non-seized servers had a larger impact than any of us expected! All non-seized servers were unreachable from our multiple vantage points.

The Community

When fighting online threats, it is rarely the case that people or companies act alone. Alone, we can only get so far. Threat actors do not act alone and neither do defenders. Team Cymru operates with community engagement central to its purpose.

This effort exemplifies the community impact. There are so many people that contributed to this effort, so many people that choose to go unnamed. One of the larger groups with a critical role in this effort used to have a banner of “Altruistic Meritocracy”. The merit, my friends, is tremendous. And the altruism is inspiring.

The Impact

Emotet is a complicated botnet to take over. Its infrastructure is redundant and fault tolerant. It is set up with distinct tiers and has some separation to further increase resiliency. Hacked servers make up most of its infrastructure. These servers are globally distributed. Before Tuesday, January 26, 2021, this model was top notch for criminal infrastructure.

Now the actors are wearing some shiny new handcuffs. The infrastructure is in law enforcement control. Fewer victims are connecting to actor-controlled systems. More people are safe today.

Information security is a war, not a battle. Crime is a human reality and the Internet is subject to these maligned human interests. But this is a success story, a win for those fighting to protect innocent victims.

Today we celebrate.