CARIS2 Statement of Interest

Tim April, Principal Architect
Information Security, Akamai Technologies

December 13, 2018

My role at Akamai includes responsibility for coordinating with external parties in different companies, organizations and governments to facilitate collaboration related to network security and attack response. This work involves interacting with trust groups as well as personal relationships with many members of the community, built over many years of working in cooperation. Below I discuss a sharing group that was setup in the wake of the initial Mirai attacks and how it continues to operate. CARIS2 would be a good venue to have a more in-depth conversation about this group and how to expand on the work that we have been doing with it for the last two years.

When the first large Mirai attacks hit [Kre16] in September of 2016, the primary method to communicate with operators and responders from other companies for attack response was via email, SMS and, occasionally, telephone. When this event occurred, I was directly involved with the response internal to Akamai, and led the external coordination with entities outside the company.

In the time between the decision and action of removing the pro-bono customer, I started to contact trusted contacts who could help or might need to know what was happening. This began with some of the ISPs impacted during the attack to let them know that the target was going to be moving. After the ISPs, I talked to some of the other large infrastructure companies to let them know of what we saw, in the event that they were targeted. The goal of this notification was to give everyone that might be impacted a heads up, so they could make preparations and brace for possible follow up attacks.

When doing the initial notifications and follow up work, phone, SMS, and email were the primary forms of communication. This approach was cumbersome and took significant effort to keep everyone on the same page. On September 23rd, two days after the the initial attacks ended, the real time communication group known as NetSecWarriors (often referred to as NSW) was created by a colleague working at one of the notified ISPs, inviting the current response team into the chat tool. We started a group that has persisted and thrived, still going today.

At its creation, NetSecWarriors was intended to be a real time group communication channel for the people involved in the Mirai response, to lower the management overhead for planning and hunting. At the start, rules and guidelines for how the participants should operate were few and far between. We relied on informal information sharing using Traffic Light Protocol and "FriendDA" (aka: we know and trust each other not to share with untrusted people, and to act on anything you can). The group with this model grew rapidly to roughly 20 people from nearly 20 organizations. Expansion was driven by pulling in people that the existing members of the group had worked with and trusted. This model lasted for a few days, until the attacks died down and the target was running on another service provider.

During this lull, the creator of the group enlisted three additional members and began the conversation around how to add some form of structure to the group. The new goal was to help nurture the current efforts, while also bringing others in to help the cause. That group formed an admin committee for the group, and drafted the first charter to govern

default content classification (TLP:Red), new member nomination and vetting, a code of conduct, and basic rules for participation. The charter was drafted to be a living document, leaving room to revise it for the future needs of the group. A primary goal was to keep the group growth controlled so members could feel comfortable sharing and working together.

Over the two years since this group's creation, multiple ad-hoc teams have been formed to address a variety of threats. This includes combatting malware campaigns, large DDoS attacks, crypto-locker outbreaks, and mass compromises. The membership of the group has steadily grown. A number of guests have been invited to sub-sections of the group to provide unique expertise, and, sometimes, these guest were promoted to full members. This same model has also been adopted by a handful of other groups, more focused on other, specific, topic areas. The NSW charter has been used as a model and modified to the needs of these new groups.

So far, NetSecWarriors has been a successful experiment in cross organizational coordination for Internet-wide and other large scale events. The members have collaborated, sharing research, real time threat information and other insights to try and make the internet a safer place for all of its users.

Thank you for your consideration.

References

[Kre16] Krebs, Brian: *KrebsOnSecurity Hit With Record DDoS*. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/. Version: September 2016