SaTC: TTP: Small: STINGAR - Deployment of highly automated, reliable, and fast cybersecurity threat response systems (1815691)

John Board PI, Tracy Futhey Co-PI – Duke University

https://stingar.security.duke.edu/

- Detect and act on new cyber threats in near real time (~1 s) – automation critical
- Share threat intel with peers
- Package so lesser resourced institutions can also contribute and benefit
- Repository of threat data for cybersecurity research in addition to operational value

Highlights

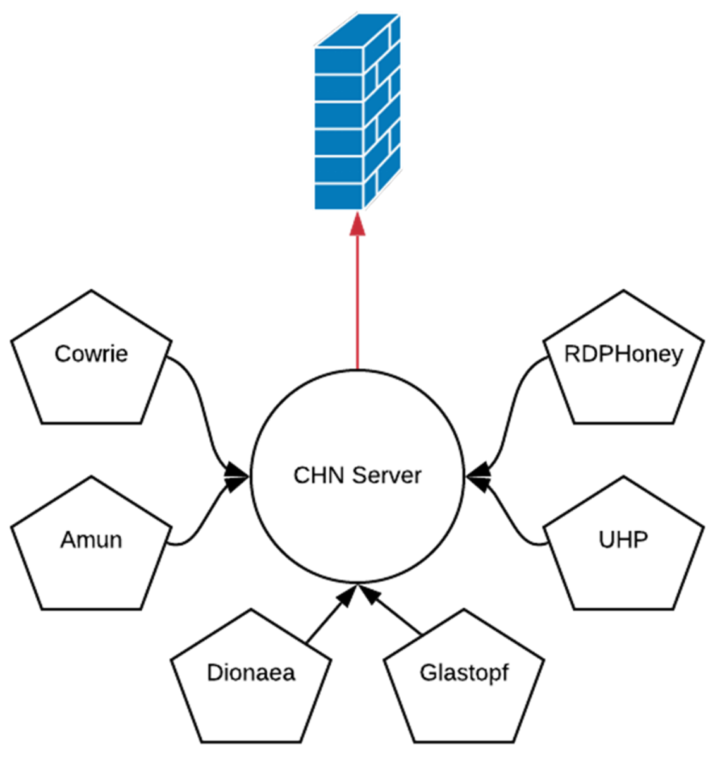
2016: Commercial campus network protection tools were costly and too slow (30min-24hr to block new threats).

Expectation that higher ed sector has systemic attackers so shared threat intel would be valuable

Day 1 in 2017 with alpha tools at one campus, no sharing – 10M blocks per day increased to >2B blocks per day (height of Mirai Botnet) – steady state of 250M/day; 85% reduction in IPS alerts.

First partner deployments: surprising fraction of attackers are unique to each institution, but many attacks do hit multiple institutions, validating sharing approach

Now: 16 partners, sharing 17K unique attacker IP addresses per day



Cowrie

RDPHoney

CHN Server

Amun

UHP

Dionaea

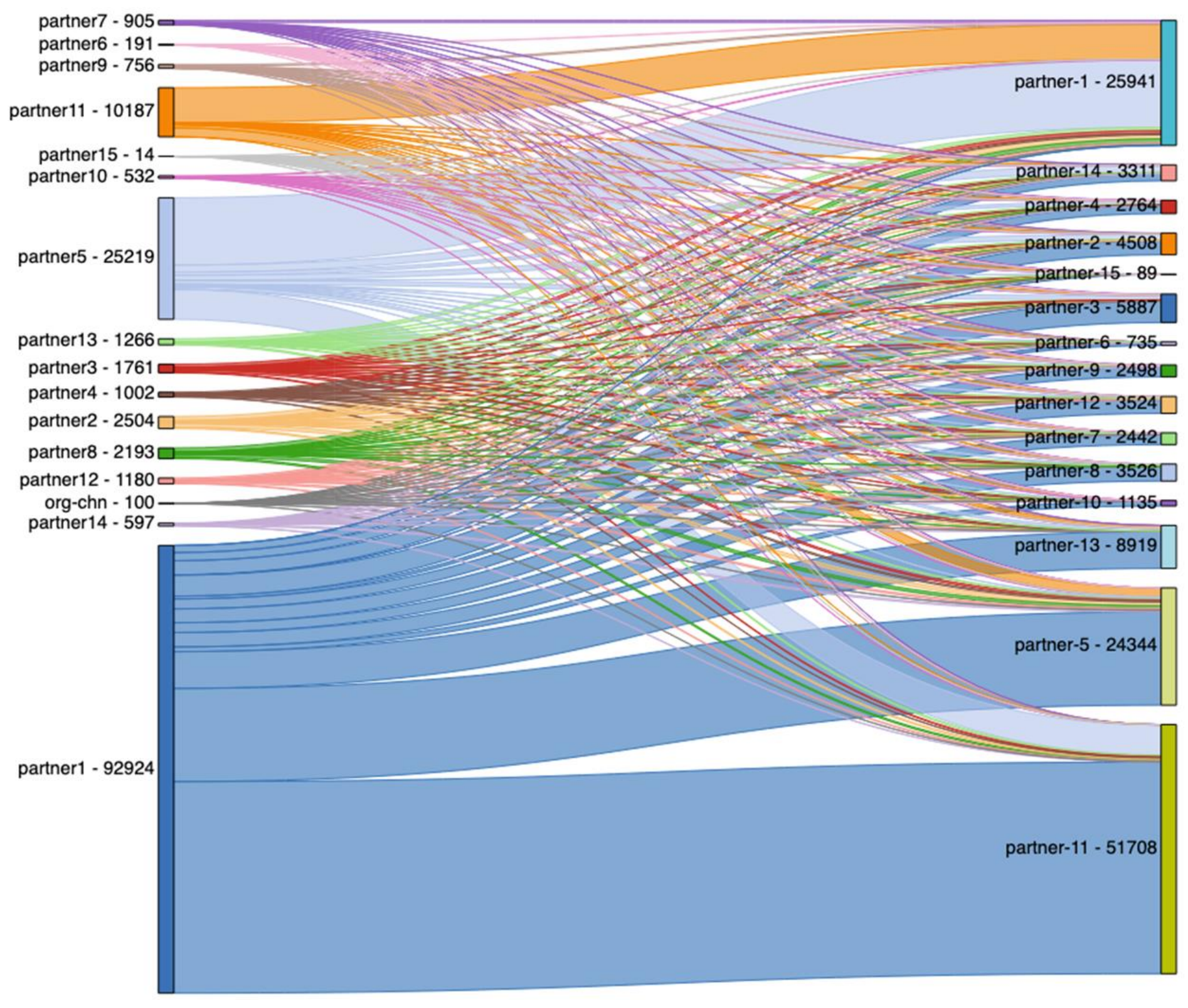
Glastopf

Expanding variety of honeypots, each targeted to specific kinds of attacks

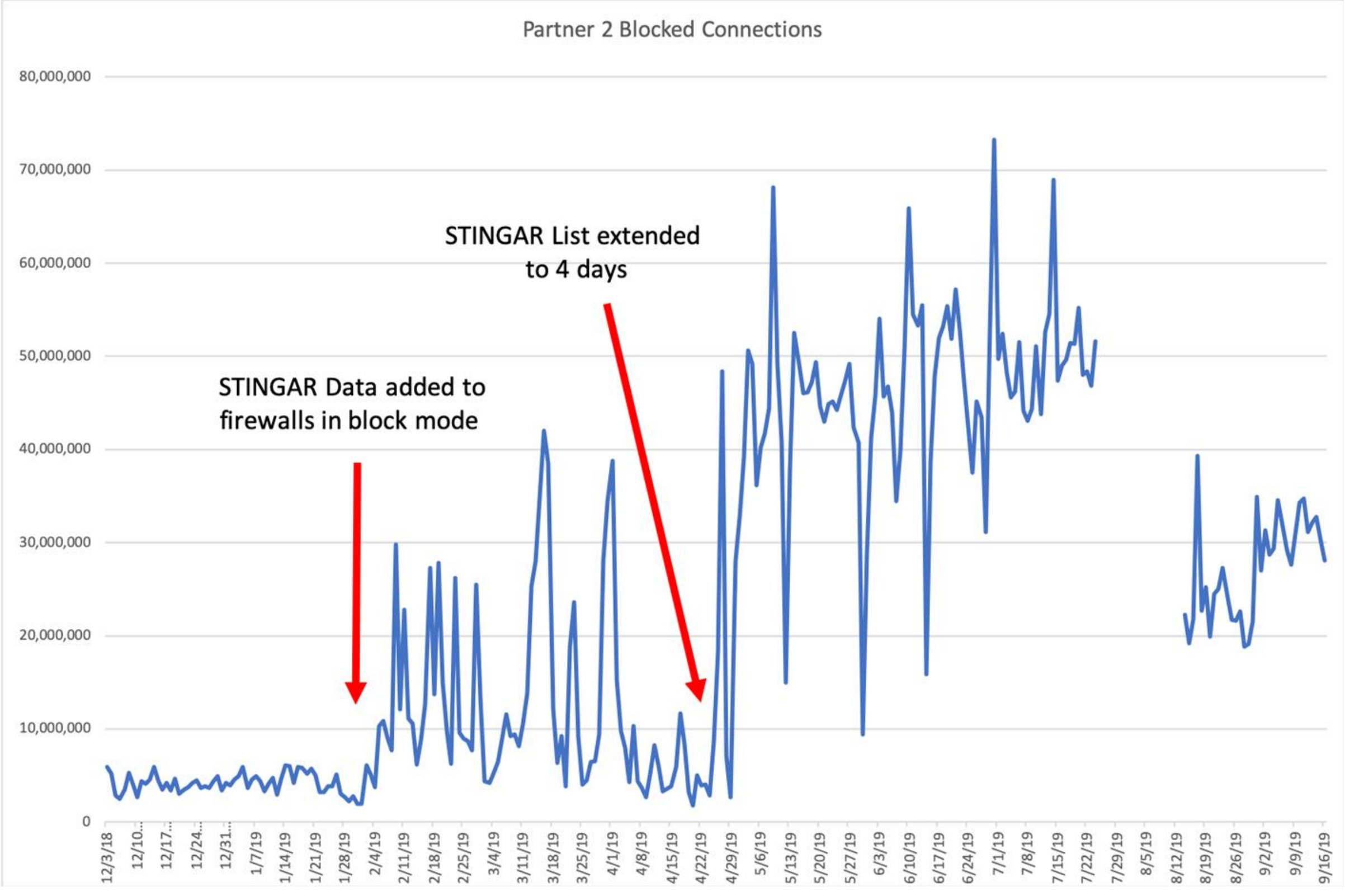
STINGAR supports a general sensor/actuator framework, but deception technology (honeypots) are primary sensors today

Back end interfaces to firewalls, edge routers (black hole routing), IPS/IDS to enable variety of protection strategies

At Duke, typically BHR rule for immediate blocking, replaced by IPS rule in 30 minutes or so to conserve finite routing table space



16 partners: seen first on left, shared and seen to right



Partner 2 Blocked Connections

STINGAR List extended to 4 days

STINGAR Data added to firewalls in block mode

Partner 2: small MSI, first switching on threats detected locally, then adding additional threats detected first by Duke

Sharing works: each new partner adds value to all existing partners

Partners large and small see immediate blocking benefits, more when sharing activated

Broader Impact - protections

Cybersecurity threats are a fact of modern life for all institutions. Higher education institutions, with the added challenge of traditions of openness, decentralization, diversity in infrastructure, and support for experimentation, represent particularly difficult challenges for cybersecurity; they are frequently viewed as soft targets by attackers. Many attacks against higher education are systemic, in the sense that attackers will move from one institution to the next with similar tactics. Smaller institutions in particular can rarely afford to hire large, high-capability cybersecurity teams, increasing their vulnerability further.

Broader Impact – other institutions, especially lesser resourced institutions

We seek to improve cybersecurity for many more institutions by creating easily shareable versions of this toolset that can be readily deployed on campuses small and large without needing deep expertise in their construction. The result will be greatly enhanced security for individual campuses, and in later stages of this project for cooperating groups of campuses who choose to share their threat data

Broader Impact – cybersecurity research data trove

Beyond operational use of collected threat data, the attack data collected in both individual and federated instances of the toolset will also create a treasure trove of actual events of great interest to cybersecurity researchers. Our hope is that better understanding of patterns in attacks and the evolving nature of commands, payloads, and C&C networks used by attackers will lead to improved security for all.

The 4th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2019 SaTC PI Meeting)
October 28-29, 2019 | Alexandria, Virginia